

STAT CONF
11/29/94
C @ 2pm

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

FILED

JUL 27 1994

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

filed
W

In the United States District Court
for the Northern District of California

Civil Action File No.

Assigned to Judge

Category 410, Antitrust

C - 94 20512 SW

PVT

ROGER SCHLAFLY, an individual, Plaintiff
v.
PUBLIC KEY PARTNERS,

Complete

COMPLAINT

and
RSA DATA SECURITY INC., Defendants.

Complaint Against Unfair Business Practices

Plaintiff makes complaint against defendants for unfair business practices, including libel, interference with contractual relationships, patent misuse, fraud, monopolization, and racketeering, and demands remedies available under federal law, including jury trial, declaratory judgment, monetary damages, and injunctive relief. Jurisdiction. The Federal Court has jurisdiction because it is based on Federal law, including antitrust and patent law. Venue is proper because defendants and plaintiff reside in this Judicial District.

COMPLAINT

1 For its complaint against defendants, plaintiff alleges as
2 follows:

3 1. This is an action for unfair business practices, libel,
4 fraud, monopolization, and racketeering by Public Key
5 Partners ("PKP"), which is managed by Mr. Robert Fougner,
6 Director of Licensing, 310 North Mary Avenue, Sunnyvale, CA
7 94086 and by RSA Data Security Inc. ("RSADSI"), which does
8 business at 100 Marine Parkway, Redwood City, CA 94065.

9 2. Plaintiff Roger Schlafly is a resident of the County of
10 Santa Cruz, State of California.

11 3. Plaintiff is in the cryptography business, and develops
12 computer software for customers. He is also a member of the
13 IEEE P1363 working group, a committee charged with adopting
14 a public key standard.

15 4. Defendant PKP is a partnership between Defendant RSA and
16 Caro-Kann Corp. of Sunnyvale. Their partnership agreement
17 is attached as Exhibit A. Mr. Jim Bidzos is the president
18 of both RSADSI and PKP. Cylink Corp. of Sunnyvale was also
19 a partner in the formation of PKP.

20 5. Federal jurisdiction is based on antitrust law (title
21 15), patent law (title 35), and racketeering law (18 USC
22 1341, 1951, 1961-1965). Request for relief is also based on
23 28 USC 1331, 1337(a), 1338(a), 1338(b), 2201, and 2202.

24 6. Defendant RSADSI is the dominant U.S. vendor of
25 cryptography software, and has monopoly power in that
26 market. It is engaged in a significant amount of interstate
27 commerce, totalling at least \$5 million per year.

28 7. Defendants have engaged in tortious interference with

1 business relationships between plaintiff and plaintiff's
2 clients, including Information Security Corp. ("ISC") and
3 AT&T.

4 8. Defendants claim to control certain patents related to
5 public key cryptography. These are the following U.S.
6 patents and their foreign equivalents.

7	Diffie-Hellman	4,200,770
	Hellman-Merkle	4,218,582
8	RSA	4,405,829
	Hellman-Pohlig	4,424,414
9	Schnorr	4,995,082

10 These PKP patents, as issued in the U.S., are attached as
11 Exhibit B. (There may also be foreign patents for Hellman-
12 Merkle and Schnorr.)

13 9. There is a substantial and continuing justiciable
14 controversy between plaintiff and defendant PKP as to PKP's
15 right to threaten or maintain suit for infringement of the
16 PKP patents, and as to the validity, scope, and enforce-
17 ability thereof, and as to whether any of plaintiff's work
18 infringes any valid claim thereof.

19 10. Plaintiff has not infringed these patents.

20 11. Plaintiff has signed a consent agreement with defendant
21 RSADSI, attached as Exhibit C. He agreed not to sell a
22 product infringing the RSA patent, except under license
23 from RSADSI or the U.S. Government. (The U.S. Government
24 funded the RSA invention, and retains certain rights.) The
25 agreement also allows plaintiff to design and manufacture
26 products using the RSA patent.

27 12. Defendant PKP sent a letter dated Jan. 12, 1994 to
28 plaintiff's client, AT&T, alleging that Digital Signature,

1 of which plaintiff is a partner, has breached the above
2 consent agreement. The letter is attached as Exhibit D.
3 In fact, no such breach has taken place. This letter was
4 written without any notification to plaintiff or Digital
5 Signature.

6 13. Defendant PKP's letter to AT&T stated:

7 ... to the extent any of AT&T's products are tainted by
8 ISC's violation of this injunction, we hereby demand that
AT&T cease their further distribution and sale.

9 The alleged violation is based on ISC's use of Digital
10 Signature software. This is a tort for PKP to send such a
11 letter, as no violation has taken place. PKP knew that
12 there was no violation because AT&T has the appropriate
13 patent licenses. Evidence that AT&T already had a license
14 is in Exhibit E, a letter from Jim Bidzos to the editor of
15 Scientific American.

16 14. Defendants' allegations have damaged plaintiff's
17 reputation, hindered his ability to sell his services, and
18 interfered with his business relationships.

19 15. Defendant PKP has mailed a letter dated April 4, 1994
20 to ISC referring to the "apparent breach of the November 15,
21 1988, Consent Judgement [sic]". The letter is attached as
22 Exhibit F. Plaintiff denies any such breach.

23 16. Plaintiff sent a letter to PKP protesting its libelous
24 actions and demanding a retraction. The letter was sent on
25 April 4, 1994 and attached as Exhibit G.

26 17. In a letter from PKP dated April 18, 1994 and attached
27 as Exhibit H, PKP refused to retract its earlier libel. The
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

letter also states that

The practice of the DSA is described in the Hellman-Diffie, Hellman-Merkle and Schnorr patents ...

This statement is obviously false, since the DSA patent application was filed after all of those other patents issued. Plaintiff's response is attached as Exhibit I. 18. Defendants have negotiated in bad faith, claiming to offer licenses but giving the run-around on terms and details. Plaintiff relied on defendants' promises that patent licenses would be available, and then lost business when PKP reneged on those promises. Copies of some correspondence with PKP on licensing is attached as Exhibit J. Plaintiff has never able to determine even what the PKP licensing policy is.

19. Defendants have fraudulently induced standards-making bodies, including American National Standards Institute ("ANSI") and Institute of Electrical and Electronics Engineers ("IEEE"), to draft standards based on the RSA and Diffie-Hellman patents by promising a reasonable and nondiscriminatory licensing policy, when in fact no such policy exists. ANSI and IEEE require such a policy, and would not have drafted RSA standards if PKP had not misrepresented its intentions.

20. Defendant PKP sent a letter dated March 15, 1991 to the American Bankers Association (in affiliation with ANSI) stating that "PKP has not denied a license to any party." A copy is attached as Exhibit K. Plaintiff was denied a license in 1990.

1 21. Plaintiff is informed and believes and on that basis
2 alleges that ISC and other parties were also denied PKP
3 licenses. Numerous users of Pretty Good Privacy ("PGP"), a
4 widely used cryptography program, have complained about
5 being denied PKP licenses.

6 22. A letter from PKP to ISC denying it an RSA license is
7 attached as Exhibit F.

8 23. Plaintiff is informed and believes and on that basis
9 alleges that defendant RSADSI attempted to rescind licenses
10 granted for use of RSAREF, one of its products, even though
11 the license agreement clearly states that the license is
12 perpetual.

13 24. By getting their technology to be declared a draft
14 standard, RSADSI has unfairly monopolized the cryptography
15 market. Plaintiff has been damaged because competing
16 technologies are regarded as nonstandard by the public.

17 25. Defendants' patent threats and fraudulent promises have
18 prevented ANSI and IEEE from adopting public key standards,
19 to the detriment of all others in the industry, including
20 plaintiff.

21 26. Plaintiff and others on standards committees have
22 invested valuable time and effort to develop a public key
23 standard, but have been thwarted by defendant PKP's patent
24 threats and fraudulent promises.

25 27. Plaintiff is informed and believes and on that basis
26 alleges that defendants have made hostile and unwarranted
27 threats against potential customers and clients of plaintiff,
28 including representatives of the U.S. Army. These threats

1 have included false assertions that ISC software is illegal
2 because of patent problems. (Even if the defendants' patent
3 claims were valid, the U.S. Army has a license to use the
4 patents anyway.)

5 28. Plaintiff is informed and believes and on that basis
6 alleges that defendants have vindictively harassed
7 competitors, including trying to promote a federal criminal
8 investigation of the author of PGP.

9 29. The U.S. Dept. of Commerce has made a determination that
10 practice of the Digital Signature Algorithm ("DSA") does not
11 infringe PKP patents. Public notice to that effect has
12 appeared in Federal Register vol. 56, no. 169, August 30,
13 1991, pp. 42980-42982, and Federal Register vol. 59, no. 96,
14 May 19, 1994, pp. 26208-26211. Copies are attached as
15 Exhibits L and M. A copy of the DSA patent is attached as
16 Exhibit N.

17 30. Defendant PKP wrote a letter to the National Institute
18 of Standards of Technology ("NIST") claiming that the DSA
19 infringes PKP patents. The letter was dated Nov. 20, 1991
20 and attached as Exhibit O. No PKP argument regarding the
21 nature of the infringement was ever made public. U.S.
22 patent 5,231,668 was issued and assigned to the United States
23 on July 27, 1993.

24 31. When the DSA was adopted by NIST as the federal Digital
25 Signature Standard, defendants publicly threatened to sue
26 anyone who uses it. These threats were conveyed to the news
27 media for the purpose of intimidating competitors, and the
28 threats were widely disseminated. A copy of a typical story

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

in the trade press is attached as Exhibit P.

32. Defendants have attempted to intimidate ANSI and IEEE not to adopt a DSA standard, based on patent claims they know to be invalid. A copy of a PKP letter is attached as Exhibit Q. They hoped to kill a DSA standard in order to monopolize the market with an RSA standard.

33. Defendant PKP has pooled patents in an attempt to monopolize public key technologies. The Hellman patents were originally issued to Stanford University and exclusively licensed to Cylink. Cylink apparently controls Caro-Kann Corp., a partner in defendant PKP. The RSA patent was originally issued to Massachusetts Institute of Technology and exclusively licensed to RSADSI. The Schnorr patent was issued to Klaus Schnorr, a German citizen who had no connection with PKP. The patents are not blocking. All are now under the exclusive licensing control of PKP.

34. Defendants have exaggerated the scope of their patents. In a publicly distributed letter dated April 20, 1990, PKP claimed:

These patents cover all known methods of practicing the art of Public Key, including the variations collectively known as El Gamal [sic].

The letter is attached as Exhibit R. PKP knows that this claim is false, but makes it anyway to intimidate competitors.

35. Defendant PKP sent a threatening letter, attached as Exhibit S, to ISC claiming that any use of public key technology must necessarily infringe PKP patents.

36. The idea of public key cryptography and digital

1 signatures is disclosed in a paper titled "Multiuser
2 cryptographic techniques" by Whitfield Diffie and Martin E
3 Hellman, National Computer Conference, vol. 45, 1976. The
4 paper was presented at a public conference in mid-June 1976,
5 and published as part of the conference proceedings shortly
6 thereafter. This was more than one year before any patents
7 were filed, and therefore in the public domain according to
8 35 USC 102(b). A copy of the paper is attached as Exhibit T.
9 37. Another paper by Diffie and Hellman, "New Directions in
10 Cryptography", IEEE Transactions on Information Theory, vol.
11 IT-22, no. 6, Nov. 1976, was submitted on June 3, 1976. It
12 discloses the public key distribution system of the Diffie-
13 Hellman patent. A copy of the paper is attached as Exhibit U.
14 38. A survey paper, "The First Ten Years of Public-Key
15 Cryptography", was published by Diffie in Proceedings of the
16 IEEE, vol. 76, no. 5, May 1988. A copy of the paper is
17 attached as Exhibit V. It states on p. 563 that Exhibit U
18 was publicly distributed in June 1976 and publicly disclosed
19 at the National Computer Conference, also in June 1976. The
20 Diffie-Hellman patent was filed on Sept. 6, 1977. This was
21 more than one year later, and hence the patent is invalid
22 and unenforceable according to 35 USC 102(b).

23 39. The Hellman-Merkle patent is invalid and unenforceable
24 because it is inoperative as disclosed. Claims 1-6 and 14-
25 17 require a quantity computationally infeasible to generate
26 from a public key. Claims 1-3 and 6-17 require secure
27 communication over an insecure channel. There are no other
28 claims. While the inventors probably believed that their

1 invention met these requirements at the time they filed
2 their patent application, it was later proved that the
3 invention does not meet the requirements. According to
4 Exhibit V pp. 565-566, it turned out to be feasible to
5 compute the secret key from the public key. It follows that
6 the claimed computational infeasibility is not achieved, and
7 the communication is not secure. In fact, according to
8 Exhibit V, the inventor had to pay a \$100 bet when the
9 invention was proved to be useless.

10 40. RSADSI has known the Hellman-Merkle invention to be
11 worthless since at least 1985, and have not used it in its
12 commercial products for that reason.

13 41. The Hellman-Merkle invention is not useful because of
14 the flaws cited in Exhibit V, and therefore fails to satisfy
15 the 35 USC 101 requirements for patent protection.

16 42. The Hellman-Pohlig patent is not even a public key
17 patent. PKP deceptively cites it to bolster their claim to
18 own all public key technology.

19 43. Defendants have claimed that ElGamal encryption, as
20 described in T. ElGamal, A Public Key Cryptosystem and a
21 Signature Scheme Based on Discrete Logarithm, IEEE
22 Transactions on Information Theory, IT-31 (no. 4, July 1985)
23 pp. 469-472, or as implemented in SecretAgent (a product of
24 ISC which uses software licensed from plaintiff), or as
25 currently being considered by the IEEE P1363 committee,
26 infringes PKP patents. Plaintiff asserts that there is no
27 infringement, even if the PKP patents are valid.

28 44. ISC had kept SecretAgent out of the commercial (non-

1 government) market for a couple of years because of PKP
2 patent claims on ElGamal encryption.

3 45. Plaintiff has suffered lost royalties as a result of
4 defendants claiming that SecretAgent infringes PKP patents.

5 46. The RSA patent claims preempt a mathematical formula,
6 and hence fail to pass the Freeman-Walter-Abele two-step
7 test for statutory subject matter under 35 USC 101. While
8 such a rejection had been made by the examiner, it was
9 traversed with the disingenuous argument that the apparent
10 formula is not a mathematical formula because it uses an
11 equivalence relation. The argument from the RSA patent file
12 wrapper is attached as Exhibit W. Plaintiff alleges that
13 this argument is mathematically incorrect.

14 47. Defendants have demanded licenses for use of the "RSA
15 algorithm" even though such a demand is prohibited by the
16 doctrine of file wrapper estoppel. Exhibit W emphatically
17 says,

18 However, there are no mathematical algorithms in the
19 applicants' claims.

20 An example of a statement that the RSA algorithm is patented
21 can be found in Bidzos's letter of Sept. 16, 1986, included
22 in Exhibit J.

23 48. Cylink has filed court papers, attached as Exhibit X,
24 stating that it believes the RSA patent to be invalid. If
25 so, PKP has knowingly extracted license fees and sued
26 competitors based on an invalid patent.

27 49. According to item 13 of Exhibit X, it appears that
28 RSADSI has denied an RSA license to Cylink.

1 50. Plaintiff will seek leave of court to amend this
2 complaint to assert such additional grounds for invalidity
3 as may be ascertained and shall give notice prior to trial
4 as may be required by 35 USC 282 of the matters specified
5 herein.

6 51. Defendant PKP acquired the Schnorr patent in a willful
7 attempt to maintain its monopoly over public key technology.
8 When use of the DSA appeared to be a non-infringing use of
9 public key, RSADSI publicly attacked DSA technology as
10 inferior, showed little interest in marketing DSA products,
11 but acquired the Schnorr patent anyway in a predatory
12 attempt to deter others from using the DSA. An example of
13 Bidzos's public disparagement of the DSA (where it is
14 referred to as the DSS) is attached as Exhibit Y.

15 52. Plaintiff is informed and believes and on that basis
16 alleges that PKP ties licensing of its patents to the
17 purchase of software and services from RSADSI, in an attempt
18 to broaden the scope of its patents and monopolize the
19 market for certain related software and services.

20 53. Defendants have organized an illegal secondary boycott
21 of competitors. RSADSI has publicly distributed a "Sink
22 Clipper" poster which urges people to boycott companies
23 selling products based on a cryptographic technology other
24 than that sold by RSADSI. It says:

25 What you can do ... Boycott Clipper devices and the
26 companies which make them exclusively: Don't buy anything
with a Clipper chip in it.

27 A copy of the text on the poster is attached as Exhibit Z.

28 54. Plaintiff has been developing software for the Tessera

1 card, a device with Clipper chip technology. Plaintiff
2 stands to suffer injury from RSADSI's secondary boycott if
3 it kills the market for Tessera cards.

4 55. Defendants' conduct and tactics with regard to the PKP
5 patents constitute patent misuse.

6 56. Plaintiff is informed and believes and on that basis
7 alleges that defendants charge different royalties to
8 different licensees, and use price discrimination to bolster
9 their monopoly.

10 57. Defendants are in violation of antitrust laws with their
11 monopolization tactics.

12 58. Defendants have defamed plaintiff by making allegations
13 of patent infringement to third parties, in violation of
14 libel laws and laws against unfair business practices.

15 59. Defendants concocted a joint scheme to fraudulently
16 exaggerate the scope of their patents and deceive standards-
17 making bodies into drafting an RSA standard on or about
18 April 6, 1990, the day the PKP partnership agreement in
19 Exhibit A was consummated. Defendants formed an association
20 -in-fact that constituted an "enterprise" within the meaning
21 of 18 USC 1961(4).

22 60. Defendants intended to use the exaggerated patents and
23 phony license promises to monopolize the public key
24 cryptography market, with full knowledge of the ANSI and
25 IEEE patent policies and of the invalidity of the Hellman-
26 Merkle patent.

27 61. Several of defendants' threats and fraudulent patent
28 claims and threats were transmitted through the U.S. Mail,

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

thus constituting mail fraud in violation of 18 USC 1341.

One such letter, Exhibit R, was sent by registered mail on or about April 20, 1990.

62. PKP also sent Exhibits K and Q through the U.S. mail system.

63. Defendants have interfered with commerce, in violation of 18 USC 1951, with their predatory tactics, unwarranted threats, and other unfair business practices.

64. Plaintiff is informed and believes and on that basis alleges that defendants have engaged in extortion by using the threat of lawsuit to extract patent licensing fees, when in fact they knew the patent to be invalid.

65. Plaintiff has been damaged, as have others, by defendants' fraud, extortion, and interference with commerce.

66. Defendant PKP has conspired with defendant RSADSI to engage in a pattern of racketeering, in violation of the Racketeer Influenced and Corrupt Organizations (RICO) Act.

67. Plaintiff damages, in lost sales, contracts, and royalties, are estimated at \$2 million. Much of this would have been interstate commerce, including royalties from ISC in Illinois.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

WHEREFORE, plaintiff prays for judgment as follows:

1. That defendants, defendants' agents, partners, servants, employees, and all others acting in concert or participating with them, be enjoined during the pendency of this action and permanently from further interference with plaintiff's business.
2. That defendants pay plaintiff \$2 million in real and punitive damages, and that damages be trebled according to antitrust and RICO laws.
3. That defendants be required to comply with the ANSI and IEEE patent policies.
4. That defendants' patent claim on all public key technology be declared invalid.
5. That practice of ElGamal encryption does not infringe any PKP patents, whether those patents are valid or not.
6. That practice of the DSA does not infringe any PKP patents, whether those patents are valid or not.
7. That the Diffie-Hellman patent be declared invalid and unenforceable.
8. That the Hellman-Merkle patent be declared invalid and unenforceable.
9. That defendants be estopped from enforcing the RSA patent.
10. That defendants be enjoined from further libeling plaintiff.
11. That defendants supply a complete list of persons and businesses that they have given false or libelous information, and that they send written retractions to each

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

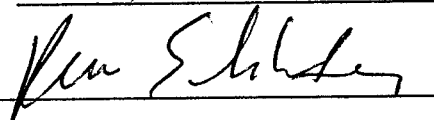
party.

12. That defendant partnership PKP be dissolved, and its patent pool be divided and returned to each patent's rightful owner.

13. That plaintiff be compensated for court costs and legal fees.

14. That plaintiff have such other and further relief as is just and proper.

Dated: July 26, 1994

By: 

Plaintiff, Roger Schlafly, Pro Se

Roger Schlafly
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

Table of Exhibits

- A. PKP partnership agreement
- B. PKP patents (U.S.)
- C. RSADSI v. Schlafly consent agreement
- D. PKP letter to AT&T
- E. Bidzos letter to Scientific American
- F. PKP letter alleging breach
- G. Schlafly letter protesting libel
- H. PKP letter refusing to retract libel
- I. Schlafly response to PKP
- J. more PKP correspondence
- K. PKP letter to ANSI committee
- L. PKP letter denying a license to ISC
- M. Federal Register announcing DSA patent-free
- N. DSA patent
- O. PKP letter to NIST alleging DSA infringement
- P. example of Bidzos threat in press
- Q. PKP letter to ANSI and IEEE with DSA threat
- R. PKP letter promising RSA licensing policy
- S. PKP letter threatening ISC
- T. early Diffie-Hellman paper
- U. famous Diffie-Hellman paper
- V. Diffie paper summarizing public key history
- W. RSA patent file wrapper excerpt
- X. Cyling complaint against RSADSI
- Y. example of Bidzos attack on DSA in press
- Z. RSADSI poster urging boycott

Exhibit A

AGREEMENT OF INTENT

This Agreement of Intent is entered into as of this 6th day of April, 1990, by and among Caro-Kann Corporation, a California Corporation having its principal place of business at 130B Kifer Court, Sunnyvale, California, 94086 ("CKC"), Cylink Corporation, a California corporation having its principal place of business at 110 S. Wolfe Road, Sunnyvale, California, 94086 (hereinafter referred to as "Cylink"), RSA, a Delaware corporation having its principal place of business at 10 Twin Dolphin Drive, Redwood City, Ca., 94065 (hereinafter referred to as "RSA").

R E C I T A L S

WHEREAS, Cylink and RSA each hold rights to certain patents in the field of encryption and decoding of telecommunications transmissions.

WHEREAS, CKC and RSA wish to form a partnership to jointly license these patents to third parties.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties to this Agreement Of Intent agree as follows:

A G R E E M E N T

ARTICLE 1

DEFINITIONS

For the purpose of this Agreement Of Intent, the following definitions shall apply:

1.1 "Affiliate" shall mean a person that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is in common control with, the person specified.

1.2 "Ancillary Agreements" shall mean the RSA License Agreement, the Cylink License Agreement and the Partnership Agreement.

1.3 "Closing" shall mean the consummation of the various transactions contemplated by Article 4 hereof which shall occur at the date, place and time agreed by the Parties in accordance with Section 4.4 hereof.

1.4 "Cylink License Agreement" shall mean that certain License Agreement in the form attached hereto as Exhibit A, which agreement shall be entered into among the Partnership, CKC and Cylink as of the Closing in accordance with Section 2.2 below.

1.5 "Licensed Rights" shall mean those patent and other industrial property rights which are to be licensed to the Partnership by RSA and Cylink pursuant to the RSA License Agreement and Cylink License Agreement, respectively.

1.6 "MIT Agreement" shall mean that certain License Agreement, dated September 29, 1983, and all amendments thereto, between RSA and the Massachusetts Institute of Technology.

1.7 "Partner" shall mean RSA or Cylink, as applicable. "Partners" shall mean RSA and Cylink.

1.8 "Partnership Agreement" shall mean that certain Partnership Agreement in the form attached hereto as Exhibit B to be entered into between RSA and CKC as of the Closing in accordance with Section 2.1 below.

1.9 "Partnership" shall mean the partnership formed pursuant to the partnership Agreement.

1.10 "RSA License Agreement" shall mean that certain License Agreement in the form attached hereto as Exhibit C, which agreement shall be entered into between the Partnership and RSA as of the Closing in accordance with Section 2.2 below.

1.11 "Stanford Agreement" shall mean that certain License Agreement, dated as of August 25, 1989 between Stanford University and Cylink.

ARTICLE 2

FORMATION AND ORGANIZATION OF THE PARTNERSHIP; EXECUTION OF ANCILLARY AGREEMENTS

2.1 Formation of the Partnership. On or before the Closing and subject to the terms and conditions herein contained, RSA and CKC shall execute and deliver the Partnership Agreement and cause the Partnership to be formed in accordance with the terms of said Partnership Agreement. Without limitation of the foregoing, RSA and CKC shall each, as of the Closing, make those capital contributions to the Partnership required by Article 3, Paragraph 1 of the Partnership Agreement.

2.2 Execution of License Agreements. On or before the Closing and subject to the terms and conditions herein contained, Cylink shall execute and deliver the Cylink License Agreement to

the Partnership, and RSA shall execute and deliver the RSA License Agreement to the Partnership.

ARTICLE 3

WARRANTIES AND REPRESENTATIONS OF THE PARTIES

3.1 Warranties of RSA. RSA hereby represents and warrants to CKC and Cylink that, at and as of the date of this Agreement and at and as of the date of the Closing, the following statements are and shall be true and correct in all material respects:

(a) Organization and Good Standing of RSA. RSA is a corporation duly organized, validly existing and in good standing under the laws of the State of Delaware and has the corporate power and authority to engage in the business RSA is presently engaged in and to enter into this Agreement and to perform its obligations hereunder.

(b) Authorization. All corporate action on the part of RSA and RSA's officers and directors necessary for the authorization, execution and delivery of this Agreement and for the performance of all of RSA's obligations hereunder has been taken and this Agreement and the Ancillary Agreements (to the extent RSA is a party thereto), when executed and delivered, shall each constitute a valid, legally binding and enforceable obligation of RSA.

(c) Government and Other Consents. No consent, authorization, license, permit, registration or approval of, or exemption or other action by, any governmental or public body or authority is required in connection with RSA's execution and delivery of this Agreement or with the performance by RSA of its obligations hereunder.

(d) Effect of Agreement. RSA's execution and delivery of this Agreement, performance of RSA's obligations hereunder and RSA's consummation of the transactions contemplated hereby will not, (i) to the best of RSA's knowledge, violate any provision of any law, statute, rule or regulation to which RSA is subject; (ii) violate any judgment, order, writ, injunction or decree of any court applicable to RSA; (iii) to the best of RSA's knowledge, have any effect on the compliance of RSA with any laws, statutes, rules, regulations, orders, decrees, licenses, permits or authorizations which would materially and adversely affect RSA; (iv) result in the breach of, or be in conflict with, any term, covenant, condition or provision of, or affect the validity, enforceability and subsistence of any agreement, lease or other commitment to which RSA is a party and which would materially and

adversely affect RSA; or (v) to the best of RSA's knowledge, result in the creation or imposition of any lien, pledge, mortgage, claim, charge, or encumbrance upon any assets of RSA.

(e) MIT Agreement. True and complete copies of the MIT Agreement have been delivered to Cylink, and there are no amendments, modifications, commitments or other understandings, written or oral, between RSA and the Massachusetts Institute of Technology pertaining to the subject matter of the MIT Agreement other than as set forth in those documents so delivered to Cylink. The MIT Agreement is valid and enforceable in accordance with its terms, and RSA is not in default in the performance of any of its obligations thereunder, and, to the best of RSA's knowledge, the Massachusetts Institute of Technology is not in default thereunder. Subject to the obtaining the consent of the Massachusetts Institute of Technology to an exclusive grant of all license rights under the MIT Agreement, including all sublicensing rights, to the Partnership, such license will not result in any breach or default by RSA of the obligations thereunder.

(f) Brokers, Finders. RSA has not retained any person to act on RSA's behalf, nor has any person contended that such person was so retained, to assist RSA as RSA's broker, finder or agent in connection with this Agreement.

(g) Disclosure. No representation or warranty by RSA contained in this Agreement and no writing, certificate, exhibit, list or other instrument required to be furnished pursuant hereto contains or will contain any untrue statement of a material fact or omits or will omit any material fact necessary in order to make the statements and information contained therein not misleading.

3.2 Warranties of CKC and Cylink. CKC and Cylink hereby represent and warrant to RSA that, at and as of the date of this Agreement and at and as of the date of the Closing, the following statements are and shall be true and correct in all material respects:

(a) Organization and Good Standing of CKC and Cylink. CKC and Cylink are corporations duly organized, validly existing and in good standing under the laws of the State of California and have the corporate power and authority to engage in this Agreement and to perform its obligations hereunder.

(b) Authorization. All corporate action on the part of CKC, Cylink, their officers and directors necessary for the authorization, execution and delivery of this Agreement and for the performance of all of its obligations hereunder has been taken and this Agreement and the Ancillary Agreements (to the extent either CKC or Cylink are parties thereto), when fully executed and delivered, shall each constitute a valid, legally binding and

enforceable obligation of CKC and/or Cylink, as the case may be.

(c) Government and Other Consents. No consent, authorization, license, permit, registration or approval of, or exemption or other action by, and governmental or public body or authority is required in connection with execution and delivery of this Agreement by CKC and Cylink or with the performance by any of their respective obligations hereunder.

(d) Effect of Agreement. CKC's and Cylink's execution and delivery of this Agreement, performance of their obligations hereunder and their consummation of the transactions contemplated hereby will not, (i) to the best of their knowledge, violate any provision of any law, statute, rule or regulation to which they are subject; (ii) violate any judgment, order, writ, injunction or decree of any court applicable to CKC or Cylink; (iii) to the best of their knowledge, have any effect on the compliance of CKC or Cylink with any laws, statutes, rules, regulations, orders, decrees, licenses, permits or authorizations which would materially and adversely affect CKC or Cylink; (iv) to the best of their knowledge, result in the breach of, or be in conflict with, any term, covenant, condition or provision of, or affect the validity, enforceability and subsistence of any agreement, lease or other commitment to which CKC or Cylink is a party and which would materially and adversely affect CKC or Cylink; or (v) to the best of their knowledge, result in the creation or imposition of any lien, pledge, mortgage, claim, charge, or encumbrance upon any assets of CKC or Cylink.

(e) Stanford Agreement. True and complete copies of the Stanford Agreement have been delivered to RSA, and there are no amendments, modifications, commitments or other understandings, written or oral, between Cylink and Stanford University pertaining to the subject matter of the License Agreement other than as set forth in those documents so delivered to RSA. The Stanford Agreement is valid and enforceable in accordance with its terms, and Cylink is not in default in the performance of any of its obligations thereunder, and, to the best of Cylink's knowledge, Stanford University is not in default thereunder. Subject to the obtaining of the consent Stanford University to an exclusive grant of all license rights under the Stanford Agreement, including all sublicensing rights, to the Partnership, such assignment will not result in any breach or default by Cylink of the obligations thereunder.

(f) Brokers, Finders. Neither CKC or Cylink has retained any person to act on its behalf, nor has any person contended that such person was so retained, to assist as its broker, finder or agent in connection with this Agreement.

(g) Disclosure. No representation or warranty by CKC or Cylink contained in this Agreement and no writing,

certificate, exhibit, list or other instrument required to be furnished pursuant hereto contains or will contain any untrue statement of a material fact or omits or will omit any material fact necessary in order to make the statements and information contained therein not misleading.

(h) CKC. CKC is a wholly owned subsidiary of Cylink.

ARTICLE 4

CONDITIONS TO CLOSING

4.1 Conditions Precedent to the Obligations of CKC and Cylink. All of the obligations of CKC and Cylink hereunder are subject to satisfaction of each of the following conditions, any or all of which may be waived, in whole or in part, by CKC and Cylink prior to or at the Closing:

(a) Representations and Warranties. The representations and warranties of RSA contained in Section 3.1 shall be true and correct at and as of the Closing, and RSA shall have delivered to CKC and Cylink a certificate of RSA, dated as of the Closing Date, to the foregoing effect duly executed by a duly authorized officer of RSA.

(b) Covenants. RSA shall have observed and performed all covenants to be observed and performed by RSA pursuant to this Agreement as of the Closing and RSA shall have delivered to CKC and Cylink a certificate of RSA, dated as of the Closing Date, to the foregoing effect duly executed by a duly authorized officer of RSA.

(c) Ancillary Agreements. The Partnership, CKC, Cylink and The Board of Trustees of the Leland Stanford University shall have executed and delivered to the Partners the Cylink License Agreement and shall have fully performed any of their obligations thereunder required to be performed by them prior to the Closing Date. The Partnership, RSA and the Massachusetts Institute of Technology shall have executed and delivered to the Partners the RSA License Agreement.

(d) Third-Party Consents. The third-party consents required to be obtained prior to the Closing, if any, shall have been so made or obtained prior to Closing, and all required waiting periods shall have expired, to the reasonable satisfaction of CKC and Cylink.

(e) No Suits, Proceedings. No suit, action, investigation, inquiry or proceeding by any person or by any governmental body, or other legal or administrative proceeding

shall have been instituted or threatened which questions the validity or legality of the transactions contemplated hereby.

4.2 Conditions Precedent to the Obligations of RSA. All of the obligations of RSA hereunder are subject to satisfaction of each of the following conditions, any or all of which may be waived, in whole or in part, by RSA prior to or at the Closing:

(a) Representations and Warranties. The representation and warranties of CKC and Cylink contained in Section 3.2 of this Agreement shall have been true and correct when made and shall be true and correct at and as of the Closing, and both CKC and Cylink shall have delivered to RSA certificates, dated as of the Closing Date, to the foregoing effect executed by duly authorized officers of CKC and Cylink.

(b) Covenants. CKC and Cylink shall have observed and performed all covenants to be observed and performed by them pursuant to this Agreement as of the Closing and both CKC and Cylink shall have delivered to RSA certificates, dated as of the Closing Date, to the foregoing effect executed by duly authorized officers of CKC and Cylink.

(c) Ancillary Agreements. The Partnership, RSA and the Massachusetts Institute of Technology shall have executed and delivered to the Partners the RSA License Agreement and shall have fully performed any of its obligations thereunder required to be performed by it prior to the Closing Date. The Partnership, CKC, Cylink and the Board of Trustees for the Leland Stanford University shall have executed and delivered to the Partners the Cylink License Agreement.

(d) Third-Party Consents. The third-party consents required to be obtained prior to the Closing, if any, shall have been so made or obtained prior to Closing, and all required waiting periods shall have expired, to the reasonable satisfaction of RSA.

(e) No Suits, Proceedings. No suit, action, investigation, inquiry or proceeding by any person or by any governmental body, or other legal or administrative proceeding shall have been instituted or threatened which questions the validity or legality of the transactions contemplated hereby.

4.3 Deliveries to Be Made at the Closing. At the Closing,

(a) Deliveries to Be Made by RSA. RSA shall deliver to the Partnership, CKC and/or Cylink, as the case may be, the following instruments in form and substance reasonably satisfactory to the Partnership, CKC, Cylink and Cylink's counsel:

(i) To the Partnership, the capital contribution of \$10,000 required to be made by Article 3, Paragraph 1 of the Partnership Agreement;

(ii) To CKC and Cylink, the officer's certificates as required by Subsections 4.1(a) and (b);

(iii) To the Partnership, any third-party consents required by Subsection 4.1(c);

(iv) To Cylink, an option to sublicense the right to make, use and sell products which would otherwise infringe on the Licensed Rights presently licensed to RSA under the MIT Agreement on terms acceptable to Cylink, which acceptance can not be unreasonably withheld.

(b) Deliveries to Be Made by CKC and Cylink. CKC and/or Cylink shall deliver to the Partnership and/or RSA, as the case may be, the following instruments in form and substance reasonably satisfactory to the Partnership, RSA and RSA's counsel:

(i) To the Partnership, CKC shall deliver the capital contribution of \$10,000 required to be made by Article 3, Paragraph 1 of the Partnership Agreement;

(ii) To RSA, CKC and Cylink shall deliver the officer's certificates required by Subsections 4.2(a) and (b); and

(iii) To RSA, CKC and Cylink shall deliver the third-party consents required by Subsection 4.2(e).

(c) Joint Deliveries. The parties and the Partnership shall execute and cause to be executed, or mutually confirm delivery of original executed copies of, the following agreements:

(i) The RSA License Agreement; and

(ii) The Cylink License Agreement.

4.4 Time and Place of Closing. Consummation of the transaction contemplated by this Agreement and the related transfers shall occur at such time and place as Cylink and RSA shall mutually agree. The Partners agree that the Closing shall be scheduled to occur on April 6, 1990, or as soon thereafter as they may agree, but not later than April 13, 1990.

4.5 Consummation of Closing. All acts, deliveries and confirmation comprising the Closing regardless of chronological sequence shall be deemed to occur contemporaneously and simultaneously upon the occurrence of the last act, delivery or confirmations and shall not be effective unless and until the last of same shall have occurred.

ARTICLE 5

GENERAL PROVISIONS

5.1 Arbitration. All disputes, controversies or differences arising out of or in relation to or in connection with this Agreement, which cannot be settled by discussion and mutual accord, shall be finally settled by arbitration. Each party shall be entitled to appoint one arbitrator, who shall not be an Affiliate, officer, director, employee, agent, vendor or contractor of that party. The appointed arbitrators shall then appoint a neutral arbitrator who shall serve as Chairman, and the arbitration shall be conducted by the arbitrators so chosen. All arbitrators so appointed shall be experienced in the business of licensing intellectual property rights, and the Chairman shall be a practicing attorney in said field. The arbitration shall be conducted in the County of Santa Clara, California. Demand for arbitration shall be made in writing and shall be served upon the party or parties to whom the demand is addressed. If the party receiving the demand for arbitration does not appoint its arbitrator within 30 days after receiving such notice, the arbitrator(s) appointed by the party or parties shall be further empowered to serve on behalf of the non-responding party. The arbitrators are authorized to award any remedy, legal or equitable, as well as any interim relief as they deem appropriate in their discretion. Application may be made to any court having jurisdiction over the proceedings to assist the arbitrators in performing their arbitral duties, to confirm their award and to enforce any such award as a judgement of said court.

5.2 Counterparts. This Agreement may be executed in any number of counterparts, and each counterpart shall constitute an original instrument, but all such separate counterparts shall constitute only one and the same instrument.

5.3 Law to Govern. The validity, construction and enforceability of this Agreement shall be governed in all respects by the law of California applicable to agreements negotiated, executed and performed in California between California corporations, whether one or more of the parties

shall be or hereafter become a resident of another state or country.

5.4 Severability. If any provision in this Agreement shall be found or be held to be invalid or unenforceable then the meaning of said provision shall be construed, to the extent feasible, so as to render the provision enforceable, and if no feasible interpretation would save such provision, it shall be severed from the remainder of this Agreement which shall remain in full force and effect unless the severed provision is essential and material to the rights or benefits received by any party. In such event, the party shall use best efforts to negotiate, in good faith, a substitute, valid and enforceable provision or agreement which most nearly effects the parties' intent in entering into this Agreement.

5.5 Subject Headings. The subject headings of the Articles and Sections of this Agreement are included for the purpose of convenience of reference only, and shall not affect the construction or interpretation of any of its provisions.

5.6 Further Assurances. The parties shall each perform such acts, execute and deliver such instruments and documents, and do all such other things as may be reasonably necessary to accomplish the transactions contemplated in this Agreement.

5.7 Expenses. Except as otherwise agreed, each party shall bear its own costs and expenses (including attorneys' fees) incurred in connection with the negotiation and preparation of this Agreement and consummation of the transactions contemplated hereby.

5.8 No Waiver. No waiver of any term or condition of this Agreement shall be valid or binding on a party unless the same shall have been mutually assented to in writing by both parties. The failure of a party to enforce at any time any of the provisions of this Agreement, or the failure to require at any time performance by one or both of the other parties of any of the provisions of this Agreement, shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of a party to enforce each and every such provision thereafter.

5.9 Assignment. This Agreement shall inure to the benefit of, and shall be binding upon, the parties and their respective successors and assigns. No party may assign or delegate this Agreement or any of its rights or duties under this Agreement without the prior written consent of the other party except as expressly set forth herein.

5.10 No Agency. Nothing contained herein or done in pursuance of this Agreement shall constitute any party the agent of the other party for any purpose or in any sense whatsoever.

IN WITNESS WHEREOF, the parties have caused this instrument to be executed by their duly authorized and empowered officers and representatives as of the day and year first above written.

CARO-KANN CORPORATION

By: Robert B. Lujan

Title: Incorporator & President

CYLINK CORPORATION

By: Jewis C Morris

Title: C.E.O

RSA DATA SECURITY, INCORPORATED

By: D James Bilzo

Title: President

GENERAL PARTNERSHIP AGREEMENT

for

PUBLIC KEY PARTNERS,
a California General Partnership

THIS GENERAL PARTNERSHIP AGREEMENT ("Agreement") is entered into as of this 6th day of April, 1990 by and between CARO-KANN CORPORATION, a California corporation having its principal place of business at 130B Kifer Court, Sunnyvale, California 94086 ("CKC"), and RSA Data Security Inc., a Delaware corporation having its principal place of business at 10 Twin Dolphin Drive, Redwood City, California, 94065 ("RSA").

NOW, THEREFORE, the parties hereto agree as follows:

ARTICLE 1 - FORMATION

1. Uniform Partnership Act; The Agreement of Intent. The parties hereby form a general partnership pursuant to the provisions of the Uniform Partnership Act as enacted in the State of California and pursuant to that certain Agreement of Intent, dated as of April 6, 1990 (the "Agreement of Intent") between RSA, Cylink Corporation ("Cylink") and CKC.

2. Name. The name of the partnership is "PUBLIC KEY PARTNERS," a California general partnership (the "Partnership").

3. Place of Business. The principal place of business for the Partnership shall be located at 130B Kifer Court, Sunnyvale, California, 94086, with a mailing address of P.O. Box _____, Palo Alto, California, until changed by designation of the Management Committee.

4. Agent for Service of Process. The initial agent for service of process for the Partnership will be Robert B. Fougner, a resident of San Mateo County, California. The agent for service of process may be changed at any time during the term of the Partnership by the President. The President shall file the Statement by Unincorporated Association of Address of Principal Office and Designation of Agent for Service of Process required by California Corporations Code Section 24003.

5. Fictitious Business Name Statement. The President shall, on the Partnership's behalf, sign and cause to be filed and published an appropriate fictitious business name statement under Section 17910 of the California Business and Professions Code within forty (40) days after the Partnership begins doing business, within forty (40) days after any subsequent change in its membership, and before the expiration of any previously filed statement.

6. Purpose. The business and purpose of the Partnership shall be to engage in the licensing to third parties of the Licensed Rights, and such other means of generating revenue for the Partners as they may elect to pursue upon Unanimous Vote of the Partners and to do all things incidental to or in furtherance of these enumerated purposes.

7. Compliance with Agreement of Intent. The Partners acknowledge and agree that the Partnership and the Partners, in their capacity as Partners of the Partnership, shall take all actions reasonably required to comply with the terms, conditions and covenants of the Agreement of Intent.

ARTICLE 2 - DEFINITIONS

1. The Agreement of Intent. Except as provided in Article 2, Paragraph 2 below, or as otherwise provided herein, the definitions set forth in the Agreement of Intent shall apply for the purposes of this Agreement.

2. Other Definitions. For the purposes of this Agreement, the following definitions shall apply:

(a) "Affiliate" shall mean any entity that is directly or indirectly controlled by, controls or under common control with a party hereto through the ownership of more than fifty percent (50%) of the outstanding stock thereof

(b) "Ancillary Agreements" shall mean the Agreement of Intent, the RSA License Agreement and the Cylink License Agreement.

(c) "Capital Account" shall mean an account maintained on the Partnership's books for each Partner strictly in accordance with the rules set forth in Treasury Regulations Section 1.704-1(b)(2)(iv). Subject to the preceding sentence, each Partner's Capital Account shall be increased by:

(1) the amount of money contributed by that Partner to the Partnership,

(2) the fair market value of any property contributed by that Partner to the Partnership (net of any liabilities secured by such contributed property that the Partnership is considered to assume or take subject to under Code Section 752), and

(3) allocations to that Partner of Profit and other items of book income and gain, including

income and gain exempt from tax and income and gain described in paragraph (b)(2)(iv)(g) of Treasury Regulations Section 1.704-1, but excluding income and gain described in paragraph(b)(4)(i) of Treasury Regulations Section 1.704-1;

and shall be decreased by:

(4) the amount of money distributed to that Partner by the Partnership,

(5) the fair market value of property distributed to that Partner by the Partnership (net of liabilities secured by such distributed property that such Partner is considered to assume or take subject to under Code Section 752),

(6) allocations to that Partner of expenditures of the Partnership of the type described in Code Section 705(a)(2)(B), and

(7) allocations of Loss and other items of book loss, including items of loss and deduction described in Treasury Regulations Section 1.704-1(b)(2)(iv)(g), but excluding items described in (6) above and paragraphs(b)(4)(i) or (b)(4)(iii) of Treasury Regulations Section 1.704-1,

and shall otherwise be adjusted in accordance with the additional rules set forth in Treasury Regulations Section 1.704-1(b)(2)(iv).

(d) "Capital Contribution" shall mean the money contributed by the Partners to the Partnership in exchange for their interests in the Partnership in accordance with Article 3, Paragraph 1 below.

(e) "Code" shall mean the Internal Revenue Code of 1986, as amended from time to time.

(f) "Cylink License Agreement" shall mean that certain License Agreement entered into among the Partnership, CKC, Cylink Corporation and The Board Of Trustees of the Leland Stanford University.

(g) "Licensed Rights" shall mean those patent and other industrial property rights which are licensed to the Partnership under the Cylink License Agreement and the RSA License Agreement.

(h) "Licensing Committee" shall consist of those persons appointed by the Partners pursuant to Article 6, Paragraph 4 hereof and, subject to said Article 6, Paragraph 4,

shall be responsible for approval of the terms upon which the Licensed Rights are licensed by the Partnership to third parties.

(i) "Management Committee" shall mean that committee appointed by the Partners pursuant to Article 6, Paragraph 2 hereof.

(j) "Material Breach" shall have the meaning set forth in Article 9, Subparagraph 3(g) hereof.

(k) "MIT Agreement" shall mean the license agreement dated September 23, 1983, between the Massachusetts Institute of Technology and RSA, and the letter amendments thereto dated May 20, 1986 and January 29, 1988.

(l) "Profit" and "Loss" shall mean, for each taxable year, the Partnership's net taxable income or net taxable loss for such taxable year, as determined under Section 703(a) of the Code with the following adjustments:

(1) Any tax-exempt income, as described in Section 705(a)(1)(B) of the Code, shall be taken into account in computing such taxable income or taxable loss as if it were taxable income.

(2) Any expenditures of the Partnership described (or treated as described) in Section 705(a)(2)(B) of the Code for such taxable year, shall be taken into account in computing such taxable income or taxable loss as if they were deductible items.

(3) Any items allocated under Article 4, Paragraph 2 shall not be taken into account in computing such taxable income or taxable loss.

(4) In lieu of any depreciation, amortization and other cost recovery deductions taken into account in computing such taxable income or loss, the Partnership shall compute such deductions based on the book value in accordance with Treasury Regulations Section 1.704-1(b)(2)(iv)(g)(3).

(5) Gain or loss resulting from any disposition of Partnership property with respect to which gain or loss is recognized for federal income tax purposes shall be computed by reference to the book value of the property disposed of, notwithstanding that the adjusted tax basis of such property may differ from its book value.

(6) "Book value" as used herein means, as of any particular date, the value at which any asset of the Partnership is properly reflected on the books of the

Partnership as of such date in accordance with the Treasury Regulations Section 1.704-1(b). The book value of all Partnership assets may, if the Partners agree, be adjusted to equal their respective gross fair market values, as determined by independent appraisal, at the times specified in such Treasury Regulations.

(m) "Partner(s)" shall mean RSA and CKC in their capacities as general partners of the Partnership.

(n) "President" shall mean Mr. D. James Bidzos, or such other individual as may be hereafter designated by the Management Committee pursuant to Article 6, Paragraph 1 below, to be responsible for the day-to-day operations of the Partnership and for the various actions specifically required herein to be performed by the President.

(o) "RSA License Agreement" shall mean that certain license agreement entered into among the Partnership, RSA and the Massachusetts Institute of Technology.

(p) "Stanford Agreement" shall mean that certain license agreement dated August 25, 1989 between Cylink Corporation and the Board of Trustees of the Leland Stanford University.

(q) "Terminating Event" shall have the meaning set forth in Article 9, Paragraph 3 hereof.

(r) "Termination by Dissolution" and "Termination by Purchase" shall each have the meaning set forth in Article 9, Paragraph 1 hereof.

(s) "Unanimous Vote of the Partners" shall mean an affirmative, unanimous written vote by the Partners.

ARTICLE 3 - PARTNERSHIP INTEREST AND CAPITAL

1. Capital Contributions of CKC and RSA. CKC and RSA each shall be obligated, severally and not jointly, to contribute the sum of ten thousand dollars (\$10,000) to the Partnership for an aggregate Capital Contribution by them of twenty thousand dollars (\$20,000) to the Partnership. The Capital Contributions by CKC and RSA shall be made to the Partnership on or before the Closing.

2. Excess Partnership Debts. Upon liquidation of the Partnership each of the Partners shall make additional capital contributions in an aggregate amount equal to that required to pay any debts and obligations of the Partnership to the extent that application of Partnership assets in accordance with Article 5, Subparagraph 2(a) hereof is insufficient to satisfy all such

Partnership debts and obligations. Such payments by the Partners shall be equal to the negative balance of their respective Capital Accounts, after valuing all of the Partnership assets and calculating any additional Profits or Losses, until each Capital Account is restored to zero and thereafter in equal amounts until all such debts and obligations are paid.

3. Interest on and Return of Capital Contributions. No interest shall be paid on any Capital Contribution to the Partnership. Except as otherwise specifically provided in this Agreement, no Partner shall be entitled to a return of any portion of that Partner's Capital Contribution at any time during the term of the Partnership or until the dissolution and liquidation of the Partnership has been completed.

4. Property of the Partnership. All property originally paid, contributed, or transferred to the Partnership as Capital Contributions of the Partners or subsequently acquired by the Partnership by purchase or otherwise, shall be the sole property of the Partnership.

ARTICLE 4 - ALLOCATIONS OF PROFITS AND LOSSES

1. General Allocation. The Profits and Losses of the Partnership shall be allocated amongst the Partners as follows:

(a) Loss Allocation. Losses of the Partnership shall be allocated 50% to CKC and 50% to RSA.

(b) Profits Allocation. Profits of the Partnership shall be allocated amongst the Partners in accordance with the following priorities:

(i) Profits shall first be allocated amongst the Partners in proportion to the deficits in their Capital Accounts until such time as the balance of both Partner's accounts are restored to zero;

(ii) Profits shall then be allocated 50% to CKC and 50% to RSA until such time as the aggregate Profits allocated to the Partners pursuant to this subparagraph (b)(ii) and subparagraph (b)(i) above equal the aggregate losses allocated to the Partners pursuant to subparagraph (a), above.

(iii) Thereafter, Profits shall be allocated 65% to RSA and 35% to CKC.

(c) Profits and Losses of the Partnership shall be determined at least quarterly and at such periodic intervals as the Management Committee shall deem appropriate and upon the Partnership's liquidation. Such determination of Partnership

Profits and Losses shall be made in the same manner as for federal income tax reporting purposes by the independent certified U.S. public accountant then retained by the Partnership, whose determination shall be conclusive on both Partners.

2. Allocation of Certain Tax Items. In accordance with Treasury Regulations section 1.704-1(b)(4)(i), if any property of the Partnership is reflected in the Capital Accounts of the Partners and on the books of the Partnership at a book value that differs from the adjusted tax basis of such property, then allocations of items of income, gain, loss and deduction with respect to such property shall, strictly for federal income tax purposes, be shared among the Partners in a manner that takes account of such differences in the same manner as variations between the adjusted tax basis and fair market value of property contributed to the Partnership are taken into account in determining the Partners' share of tax items under Code Section 704(c).

3. Allocation Between Assignor and Assignee. The proportion of the income, gain, loss, deductions and credits of the Partnership for any fiscal year of the Partnership during which an interest is assigned by a Partner that is allocable in respect of such interest shall be apportioned between the assignor and the assignee of the interest on the basis of the number of days during such fiscal year that each is the owner thereof, without regard to (a) the results of Partnership operations before or after the effective date of the assignments, or (b) any distributions made to the Partners before or after the date of the assignment.

4. Allocation of Nondeductible and Unamortized Expenditures. Partnership expenditures which must be capitalized or which are not deductible shall be allocated amongst the Partners for accounting purposes in the same fashion as all other expenses of the Partnership would be allocated for the accounting period in which the expenditure was paid.

5. Allocation Of Deferred Taxable Income. Allocation of any deferred taxable income shall be based on the year in which it arose.

ARTICLE 5 - DISTRIBUTIONS

1. General Distributions. During the term of the Partnership, the Partnership shall make such distributions as shall be approved quarterly by the Management Committee in accordance with Article 6, Paragraph 2 hereof. Any such distribution during the term of the Partnership shall be made 65% to RSA and 35% to CKC.

2. Distributions on Liquidation. Upon conclusion of the Partnership term and the dissolution of the Partnership, the President shall cause the Partnership to distribute all of the Partnership's assets, properties, proceeds, profits and income in accordance with the following priorities:

(a) Payment shall first be made to satisfy all debts and obligations of the Partnership to creditors other than Partners;

(b) Payment shall then be made to satisfy all debts and obligations of the Partnership owing to Partners for other than capital and profits; and

(c) Distributions shall then be made to the Partners in an amount equal to the positive balances of their Capital Accounts (after taking into account any adjustments for the Partnership taxable year during which such liquidation occurs and after adjusting to reflect allocations that would be made if there were a taxable disposition of the Partnership's property for its fair market value). The timing and method of the distribution provided for by this Paragraph 2 shall comply with Treasury Regulations section 1.704-1(b) or any similar regulations promulgated in the future, or if no such regulations apply, as soon as possible.

In addition, upon the liquidation of any Partner's interest in the Partnership, such Partner shall be distributed an amount equal to its positive Capital Account balance at such time (after taking into account the adjustments referred to in the previous paragraph) in accordance with Treasury Regulations Section 1.704-1(b).

(d) In the event any sublicensees of the Partnership continue to owe royalties following dissolution and liquidation, they shall be collected by an agent appointed by the Partnership for this purpose, allocated and then distributed in accordance with Articles 4 and 5. CKC and RSA shall each use their best efforts to collect any royalty, sublicense payment and other fees that are owed to the Partnership.

ARTICLE 6 - MANAGEMENT

1. Authority of President. Subject to Paragraphs 2, 6, 8, 9 and 10 of this Article 6, the President shall have the authority and duty to manage all day-to-day business operations of the Partnership and the Partnership's ordinary business affairs, to assign duties and to otherwise take such action as the President deems prudent in the administration of the Partnership's affairs. The President shall prepare an annual budget for the Partnership

for each fiscal year for the term of the Partnership, which budget must be subject each year to approval by the Management Committee. The President shall be selected by the Management Committee, which shall establish the authority and responsibilities of the President and compensation to be paid to the President by the Partnership. The President may use such other titles in transacting business with third parties as the Partnership, acting through the Management Committee, and the President shall agree. The President shall be Mr. James Bidzos until such time as he resigns, fails to comply with the terms of his employment agreement or the Management Committee appoints a replacement.

2. Management Committee. The Management Committee shall meet at least quarterly and initially shall consist of four (4) members or such other even number of members as approved by a Unanimous Vote of the Partners. RSA and CKC shall each be entitled to appoint one-half of the members of the Management Committee. The Management Committee shall manage and have ultimate direction over the business and affairs of the Partnership and over the authority and responsibilities of the President. The Management Committee may act through duly noticed meetings or by its unanimous written consent. For the purpose of holding a meeting, written notice shall be given to all members not less than four (4) nor more than sixty (60) days in advance, specifying the date, time and subject matter of the meeting. Meetings of the Management Committee may be called by the President or any Partner. The Management Committee shall be authorized to act at a meeting only if a quorum is present (personally or by way of telephonic device), and a quorum shall be deemed present if members representing more than 50% of the then authorized positions on the Management Committee are present. Any action taken by the Management Committee shall require the vote by members representing more than 50% of the then authorized positions on the Management Committee. In the event any member of the Management Committee is absent from a meeting, the members of the Management Committee who are present and who were appointed by the same Partner that appointed the absent member will automatically have the right to vote on behalf of the absent member. The Management Committee shall have a Chairman duly elected by the members of the Management Committee. Notwithstanding the foregoing, the Management Committee shall not have the authority to:

(a) Do any of the acts for which a Unanimous Vote of the Partners is required pursuant to Article 6, Paragraph 6 hereof without previously obtaining such vote;

(b) Borrow any funds from or authorize any loans by the Partnership;

(c) Do or authorize any act in contravention of this Agreement; or

(d) Do any other act which would make it impossible to carry on the ordinary business of the Partnership.

3. Expansion Of The Management Committee. The Partners may hereafter unanimously agree to expand the Management Committee to five (5) members for the purpose of appointing a neutral individual unaffiliated with either Partner to serve as President and Chairman of the Management Committee. After the appointment of such individual, a quorum shall consist of at least four (4) of the then authorized positions on the Management Committee. This provision is not intended as a restriction on the Management Committee's power to appoint a new President under Paragraph 1, herein, without expanding the number of seats on the Management Committee.

4. Licensing Committee. The Licensing Committee shall consist of two members, with one each appointed by RSA and by CKC. The initial appointees of RSA and CKC shall be D. James Bidzos and Robert B. Fougner, respectively. The Licensing Committee shall act by unanimous consent by both members. Except as provided below, the Partnership shall not license any third party with respect to the Licensed Rights without prior approval by the Licensing Committee as to the terms and conditions of such licensing to that licensee. Nor shall any officer of the Partnership or either Partner deny a license to any third party without the approval of the Licensing Committee. In the event that the two members of the Licensing Committee cannot agree as to whether the Licensed Rights should be licensed by the Partnership to a particular licensee or the material terms of such license, the Management Committee shall then have authority to approve or disapprove such proposed licensing relationship and the terms thereof.

5. Obligation of Partners to Provide Skill and Time to the Partnership. Each Partner shall be obligated to apply itself diligently and to utilize its utmost skill for the business of the Partnership and shall devote as much time as is reasonably necessary for the business of the Partnership; provided, however, that no Partner, its officers, directors or employees shall be bound to devote all of their respective business time to the affairs of the Partnership, it being understood that each Partner is and will continue to be primarily engaged in other activities and in other businesses.

6. Partner Voting Rights. The Partners shall have the power to vote upon the following Partnership matters affecting, among other things, the basic structure of the Partnership, each of which shall require a Unanimous Vote of the Partners:

- (a) Amendment of the Partnership Agreement;
- (b) Any dissolution and winding up of the Partnership

other than pursuant to Article 9, Paragraphs 4, 5 and 6 hereof;

(c) Amendment of the RSA License Agreement or the Cylink License Agreement;

(d) Any change in the nature of the business conducted by the Partnership including, without limitation, the Partnership engaging in any business activity other than a sublicensing of the Licensed Rights;

(e) Admission of a new Partner;

(f) Any agreement or contract between the Partnership and a Partner or its Affiliates or the compromise and settlement of any dispute between the Partnership and a Partner or its Affiliates;

(g) Subject to Paragraph 7 below, the obtaining of capital by the Partnership in excess of those Capital Contributions of the Partners which are made pursuant to Article 3, Paragraph 1 hereof.

(i) Expansion of the Management Committee in accordance with Paragraph 3, herein.

(j) Granting sublicensing rights to any licensee, as authorized under the Cylink License and the RSA License.

7. Determinations Regarding Additional Capital. In the event that the Management Committee shall determine that the Partnership is to raise capital in excess of the amounts contributed by the Partners pursuant to Article 3, Paragraph 1 hereof, the President shall notify each of the Partners in writing of such determination. In the event the Partners elect to make any additional capital contributions, 50% of the additional capital contribution will be made by RSA and 50% of the additional capital contribution will be made by CKC, or in such other proportions as the Partners shall agree.

8. Partnership Reserve.

(a) Without limitation on Article 6, Paragraph 2 hereof, the Management Committee shall have exclusive authority to determine the amount of any cash reserves to be retained by the Partnership. The Management Committee shall cause the Partnership to retain such cash reserves as are reasonably adequate, in combination with anticipated Partnership revenue, to meet existing and contingent obligations of the Partnership.

(b) Without limitation on the Management Committee's authority to set reserves, as stated in Subparagraph 8(a), above, the partnership shall set aside a minimum of 10% of all net

Partnership profits as a reserve for anticipated operating expenses. In addition, a further reserve of 10% of all net Partnership profits shall be set aside for potential legal expenses until such reserve accumulates a total of \$500,000. All interest earned by said reserves shall be considered Partnership income.

9. Authority of Partners to Bind Partnership. Notwithstanding California Corporations Code Section 15009(1), no Partner, who is not expressly authorized to do so by the Management Committee or the Licensing Committee, as the case may be, shall be authorized or empowered to bind the Partnership with respect to any licensing or transfer of the Licensed Rights to any person or with respect to any other contractual agreement, undertaking or obligation not in the ordinary course of the Partnership's business.

10. Foreign Entities. The Partnership may establish such foreign entities and in such locations as it deems prudent to collect revenues from foreign licenses and maximize profits; although no such entities will be established without the prior written agreement of both Partners.

11. Compliance With Licenses. The Partners each agree not to cause the Partnership, either directly or indirectly through the Partnership, to breach or default with respect to any of its obligations pursuant to the RSA License Agreement and/or the Cylink License Agreement.

12. Exclusive Licensing Authority. During the term of the Partnership, the Partners will refrain from licensing their respective Licensed Rights to third parties, other than to their Affiliates, to the extent such rights have been conveyed to the Partnership under either the Cylink License or the RSA License, and provided such inaction will not breach any of the agreements specified on Attachment "B" of the RSA License or Attachment "A" of the Cylink License. In any instance when a Partner is required to enter into agreements with third parties concerning the licensing of its respective Licensed Rights to avoid breaching any pre-existing license agreements, such Partner will promptly advise the other Partner and provide sufficient information to demonstrate that it is not in breach of this Paragraph.

13. Dealings with Sublicensees. During the term of the Partnership, the Partners each agree that any contracts, product sales, business dealings or other financial relationships between either Partner and any sublicensee of the Partnership (or Affiliate of such sublicensee) shall be fully and promptly disclosed by such Partner to the other Partner. Furthermore, the Partners agree that all contacts, discussions and negotiations between PKP and any third party shall be promptly disclosed to both Partners.

14. Performance Of Licensing Obligations. CKC shall be responsible for guaranteeing performance of any and all of Cylink Corporation's obligations under the Stanford Agreement and keeping said agreement in full force and effect in accordance with its terms during the term of the Partnership and any sublicenses by the Partnership of the Licensed Rights. RSA shall be responsible for continuing to perform any and all of its obligations under the MIT License Agreement and keeping said agreement in full force and effect in accordance with its terms during the term of the Partnership and any sublicenses by the Partnership of the Licensed Rights. Without limitation on the foregoing, RSA and CKC each agree to do the following during the term of the Partnership and any sublicenses by the Partnership of the Licensed Rights:

(a) CKC will pay all amounts due Stanford under the Cylink License Agreement from the distributions received by CKC from the Partnership. RSA will pay all amounts due MIT under the RSA License Agreement from the distributions received by RSA from the partnership.

(b) CKC will immediately notify the Partnership and RSA in the event of breach of the Stanford Agreement or, upon CKC's receipt of notice of breach by Cylink Corporation, CKC will promptly take all action reasonably required to cure any such breach. RSA will immediately notify the Partnership and CKC in the event of breach of the MIT Agreement or, upon RSA's receipt of notice of breach by RSA, promptly take all action reasonably required to cure any such breach.

15. Enforcement of the Licensed Rights. In the event that the Management Committee representatives of CKC and RSA cannot agree as to whether the Partnership shall take legal action concerning infringement of the Licensed Rights by any third party, the Partner whose representatives favored such action may, at its election, take legal action independently of the Partnership at such Partner's sole expense, provided the basis for any such action concerns infringement of the Licensed Rights granted by that Partner to PKP. Furthermore, CKC and its Affiliates cannot take any action which alleges infringement of the Licensed Rights granted under the Cylink License based solely on practice of the Licensed Rights granted under the RSA License. Any damage awards or other payments obtained from such legal action shall be the sole property of the Partner that prosecuted the legal action.

ARTICLE 7 - ACCOUNTING

1. Inspection of Partnership Records. The Partnership shall keep adequate books and records at its place of business setting forth a true and accurate account of all business transactions arising out of or connected with the conduct of the Partnership business. The Partners shall have the right at all

times to have access to and to inspect and copy the Partnership books.

2. Periodic Report. Within ninety (90) days after the close of each fiscal year, the President shall cause to be prepared a financial report and shall, within said ninety (90) day period, cause a copy of the financial report to be furnished to each Partner. The copies furnished to the Partners shall include a balance sheet, income statement and cash flow statement for the Partnership as of the last day of the accounting period. The statement of income or profit and loss shall disclose the amount of any changes in income or loss and shall show in particular the amounts of depreciation, depletion, amortization, interest and extraordinary income or charges whether or not included in operating income. Within ninety (90) days following the close of the Partnership's fiscal year, the President shall further cause the Partnership's certified public accountant to compile and prepare such information as is necessary for each Partner to file its annual income tax returns and shall, during said ninety (90) day period, cause such information to be forwarded to the Partners.

3. Bank Account. The Partnership funds shall be deposited in the name of the Partnership in one or more banks to be designated by the Partners and shall be withdrawn on the signature of an authorized agent of one or more of the Partners, as the Partners shall jointly agree.

4. Fiscal Year. The fiscal year of the Partnership shall end on December 31 of each calendar year.

5. Method of Accounting. The Partnership shall use the accrual method of accounting for maintaining its financial books and records.

6. Tax Matters Partner. CKC shall be the partner responsible, at the Partnership's risk and expense, for administration of the Partnership's tax matters and accounting. All non-ministerial acts, elections and decisions by CKC on the Partnership's behalf, as well as all other non-ministerial tax and accounting decisions of the Partnership, shall be subject to the approval of both Partners.

ARTICLE 8 - ASSIGNMENT OF INTEREST

1. Voluntary Transfer of Interest. In the event a Partner wishes to sell its Partnership Interest, the selling Partner shall give written notice to the other Partner, which notice shall accompany specific evidence of the name and address of the proposed transferee, the consideration or purchase price to be paid for its Partnership Interest and all other material terms

of the proposed transfer. Subject to Article 8, Paragraph 2 below, the selling Partner shall not be permitted to sell, transfer or assign its Partnership Interest unless both: (i) the other Partner has given written approval to such sale, transfer or assignment, which approval may be given or withheld in the absolute discretion of such other Partner; and (ii) the selling Partner shall have fully complied with its obligations as to the first refusal rights of the other Partner as set forth in this Article 8, Paragraph 1. Provided the other Partner gives written approval of the sale, as required by (i), above, such other Partner shall then have an option for thirty (30) days following receipt of the selling Partner's notice to purchase all (but only all) of the offered Partnership Interest of the selling Partner at the price and on the terms stated in the notice. If the selling Partner's interest is not purchased by the other Partner and in the event that the other Partner gives its written approval to such transfer, the selling Partner may thereafter sell or transfer its Partnership Interest to the person identified in the notice at not less than the price and on the same terms stated in such notice, provided that the transferee agrees in writing prior to such transfer to become bound by all terms of this Partnership Agreement. Following such sale, the transferee shall become a substituted Partner of the Partnership. If the selling Partner is unable to sell the offered interest to the person identified in the selling Partner's original notice at the same price and on the terms as offered to the remaining Partner, the selling Partner shall, before any attempt to sell at a lower price or on more favorable terms, give the remaining Partner a new notice of election to sell in accordance with the requirements stated above and the procedure for purchase and sale shall again be followed. Following the purchase of the Partnership Interest of the selling Partner by the other Partner pursuant to this Article 8, Paragraph 1, the Partnership shall be terminated by way of a Termination by Purchase pursuant to Article 9, Paragraph 7 hereof.

2. Transfers to Affiliates. Each of the Partners shall have the right to transfer all or any portion of its interest in the Partnership to one or more of its Affiliates provided that: (i) such Affiliate agrees in writing, as a condition precedent to such transfer, to be bound by this Agreement; and (ii) following such transfer, such Affiliate and the transferor Partner shall be treated as one Partner for purposes of this Agreement hereof and shall not be permitted to vote, act or transfer their Partnership interests independently of each other for any purpose.

ARTICLE 9 - TERM AND TERMINATION

1. Term. The Partnership shall commence as of the date of this Agreement, and shall continue until expiration of the last patent, whether in the United States or elsewhere, included in the Licensed Rights, unless sooner terminated and dissolved upon the

earlier of:

(a) The date upon which the Partnership interest of one Partner is purchased by the other Partner pursuant to Article 8, Paragraph 1 hereof or this Article 9 ("Termination by Purchase");

(b) The date upon which the Partnership is dissolved and liquidated pursuant to Article 9, Paragraph 6 hereof or upon a Unanimous Vote of the Partners pursuant to Article 6, Subparagraph 6(b) hereof;

(c) The date on which the Partnership is dissolved by operation of law; provided, however, if all Partners agree prior to such event that immediately thereafter they shall reconstitute and continue the Partnership as before, then the event giving rise to a termination by operation of law shall not be deemed a Terminating Event and the Partnership shall thereafter continue.

Any termination of the Partnership pursuant to Subparagraphs (b) and (c) above, or upon natural expiration of its term, shall be referred to as a "Termination by Dissolution" for the purposes of this Partnership Agreement.

2. Withdrawal; Removal. Prior to dissolution of the Partnership, no Partner shall have the right or ability to withdraw from the Partnership. Any removal of a Partner or involuntary sale of the Partnership Interest shall be permitted only upon those terms set forth in this Article 9.

3. Terminating Events. RSA and CKC agree that each of the events set forth below shall, upon the election of the Partner(s) that is entitled to give notice with respect to such event pursuant to Article 9, Paragraph 4 below, be treated as a Terminating Event for the purposes of this Article 9:

(a) The appointment of a trustee, receiver or other custodian for all or substantially all of the property of the other Partner or for any lesser portion of such property if the result materially and adversely affects the ability of such other Partner to fulfill its affirmative or negative obligations hereunder;

(b) The filing of a petition for liquidation (and not for reorganization) in bankruptcy by the other Partner on its own behalf or the filing of any such petition against such Partner if the proceeding is not dismissed or withdrawn within sixty (60) days thereafter;

(c) An assignment by the other Partner of a substantial portion of its assets for the benefit of its creditors;

(d) The dissolution or liquidation of the other

Partner other than in consequence of a merger, amalgamation or other corporate reorganization to which it is a party;

(e) In the event a controlling interest in, or substantially all of the assets of, either Partner (or an Affiliate of such Partner that controls such Partner) is purchased or otherwise acquired by a third party.

(f) The occurrence of any of the events described in Subparagraph (a) through (d) above as to the Partnership itself;

(g) The commission of a Material Breach by a Partner.

If a Partner should suffer any event described in Subparagraphs (a) through (e), or (g) above, that Partner shall immediately advise the other Partner and the Partnership of the occurrence of such event.

For the purpose of this Agreement, the commission of any of the following acts by a Partner which is not cured within ninety (90) days following notice thereof to the breaching Partner by the other Partner or the Partnership shall constitute a Material Breach:

As to CKC, the failure by CKC to do any of the following:

(1) Timely pay all of its Capital Contributions to the Partnership in accordance with Article 3, Paragraph 1 hereof;

(2) Fully comply with its obligations contained in Article 3, Paragraph 2, Article 6, Paragraphs 11, 12 and 14 or Article 8, Paragraph 1, hereof; or

(3) Fully insure compliance by Cylink Corporation of its obligations of exclusivity contained in Article 3 of the Cylink License Agreement.

As to RSA, the failure by RSA (or its Affiliates, as applicable) to do any of the following:

(1) Timely pay all of its Capital Contributions to the Partnership in accordance with Article 3, Paragraph 1 hereof;

(2) Fully comply with its obligations contained in Article 3, Paragraph 2, Article 6, Paragraphs 11, 12 and 14, or Article 8, Paragraph 1, hereof; and

(3) Fully comply with its obligations of exclusivity under Article 2 of the RSA License Agreement.

The foregoing shall not be deemed to limit the ability of the Partnership or any Partner to seek such legal and equitable remedies as the Partnership or any such Partner shall be entitled to seek on the basis of a Material Breach by a Partner or the breach or failure of a Partner to perform any other duty or obligation not set forth above which is otherwise contained in this Partnership Agreement or the Ancillary Agreements.

4. Notice of Termination; Right to Terminate. The Partners agree that they shall each have the option, upon written notice to the Partnership and the other Partner, to declare the various events described in Article 9, Subparagraphs 3(a) through (g) above a Terminating Event and to terminate the Partnership upon the occurrence of such event as follows:

(a) As to those Terminating Events described in Article 9, Subparagraph 3(a) through (d) which pertain to the bankruptcy, or other financial problems of a Partner, the other Partner, which is not subject to such bankruptcy, or other proceedings, shall have the right to terminate;

(b) As to the Terminating Event described in Article 9, Subparagraph 3(e) involving the acquisition of a controlling interest or purchase of a substantial portion of either Partner's assets, the Partner whose interests or assets have not been acquired shall have the right to terminate.

(c) As to the Terminating Event described in Article 9, Subparagraph 3(f) which pertains to the dissolution, liquidation, bankruptcy, or other financial problems of the Partnership, each Partner shall have the right to terminate;

(d) As to the Terminating Event described in Article 9, Subparagraph 3(g) involving a Material Breach, the non-breaching Partner shall have the right to terminate.

Following the giving of said notice by a Partner, the Partners agree that the Partnership may be terminated by either a Termination by Purchase in accordance with Article 9, Paragraph 5 below or a Termination by Dissolution pursuant to Article 9, Paragraph 6 below.

5. Termination by Purchase. Upon the occurrence of a Terminating Event (other than as described in Subparagraph (b) below), RSA and CKC agree that they shall have the following rights and obligations with respect to their respective Partnership Interests:

(a) As to any Terminating Event described in Article 9, Subparagraph 3(a) through (d) hereof, the Partner which is not subject to the bankruptcy, or other proceedings described in said Article 9, Subparagraph 3(a) through (d), shall have the option to purchase the Partnership Interest of the bankrupt Partner upon the terms set forth in Subparagraph (e) below for an amount equal to the fair market value of such Interest, as determined in accordance with Subparagraph (f) below.

(b) As to any Terminating Event described in Article 9, Subparagraph 3(f), the Partnership Interests of the Partners shall not be purchased by either Partner, but rather each such Partner shall be entitled to receive such distributions, if any, from the Partnership with respect to that Partner's Partnership Interest as is distributable pursuant to Article 5, Paragraph 2 hereof or otherwise in accordance with the terms of such dissolution, liquidation, bankruptcy, or other proceeding.

(c) As to any Terminating Event described in Article 9, Subparagraph 3(e) hereof, the Partner whose interest or assets have not been purchased may, at its option, terminate the Partnership in accordance with Article 5, Paragraph 2, and Article 9, Paragraph 6, herein.

(d) As to any Terminating Event described in Article 9, Paragraph 3(g), the Partner which has not committed the Material Breach, shall have the option to purchase the Partnership Interest of the Partner which has committed the Material Breach for a total amount equal to the fair market value of such Partnership Interest, as determined in accordance with Subparagraph (f) below; provided, however, that the breaching Partner shall only be entitled to receive for its the Partnership Interest the difference between such fair market value purchase price and the amount of damages sustained by the Partnership and the non-breaching Partner as a result of such Material Breach as determined in accordance with this Subparagraph (d). In such event and in the absence of an agreement resolving such issues between the Partners, the amount of damages payable by the breaching Partner to the person to whom they shall be owing shall be determined through the arbitration procedure described in Article 12, Paragraph 1 hereof. Any payment to the breaching Partner with respect to its Partnership Interest shall be deferred until such arbitration is completed and any determination or judgment based on such arbitration has been approved in writing by all Partners or otherwise reduced to a final judgment by a court of competent jurisdiction, after appeals, if any. The amount of such damages shall be withheld by a damaged Partner as an off-set against the purchase price or paid by a purchasing Partner to a damaged Partner or the Partnership, as appropriate, and the breaching Partner shall receive the net payment, as reduced by such off-sets and payments to others, in full satisfaction of its Partnership Interest.

(e) Any rights of RSA or CKC pursuant to this Paragraph 5 to purchase the Partnership Interest of the other Partner shall be exercised, if at all, within thirty (30) days following the giving of the original notice pursuant to Article 9, Paragraph 4 above. The purchase price for a Partner's Partnership Interest shall be paid, subject to Subparagraphs (d) and (f) hereof, by a cash payment within ninety (90) days following expiration of the said thirty (30) day period.

(f) For the purpose of this Paragraph 5, the fair market value of a Partner's Partnership Interest shall be determined by arm's-length agreement between the selling Partner and the purchasing Partner. If no such agreement can be reached, the fair market value of such Interest shall be determined on the basis of the appraisal procedure as provided in this Subparagraph (f). The selling Partner and purchasing Partner shall each appoint an appraiser, and the two appraisers appointed shall in turn appoint a third appraiser. Each such appraiser shall be independent of and not an Affiliate of any of the Partners and shall be qualified to appraise the fair market value of the selling Partner's Partnership Interest. Any such appraisal shall be based on the value of the business of the Partnership as an ongoing, operational business entity, provided that the value of such interest shall be reduced by the present value of all estimated payments that the purchasing partner becomes obligated to pay, following the purchase, on behalf of the selling Partner pursuant to Subparagraph (h) below. The three appraisers shall each promptly render a good faith appraisal of the fair market value of the selling Partner's Partnership Interest. The median of the three appraisals shall be deemed to be the fair market value of such Partnership Interest. Any time periods set forth in this Paragraph 5 shall be suspended during this appraisal procedure, which shall be completed not later than sixty (60) days following expiration of the thirty (30) day period described in Subparagraph (e) above. Any such determination of fair market value pursuant to this Subparagraph (f) shall be conclusive and binding on both Partners.

(g) During any period in which a Partner has the right to purchase or is purchasing the Partnership Interest of the other Partner pursuant to this Paragraph 5, RSA and CKC shall use their best and reasonable efforts to maintain and preserve the business of the Partnership pending the consummation of such purchase.

(h) As a condition to the purchase of a selling Partner's interest pursuant to this Paragraph 5, the purchasing Partner shall assume in writing the continuing obligations of the selling Partner pursuant to the Cylink License Agreement or the RSA License Agreement, as the case may be, to make royalty, license and other payments that are payable with respect to the Licensed Rights on the basis of distributions by the Partnership.

6. Dissolution and Liquidation of the Partnership. In the event the Partners do not resolve their respective rights and obligations following the occurrence of a Terminating Event through a purchase and sale of the Partnership Interests pursuant to Paragraph 5 herein, at the option of the Partner having the right to terminate under Article 9, Paragraph 4, herein, the Partnership shall be terminated by way of a Termination by Dissolution, and RSA and Cylink shall promptly dissolve the Partnership in accordance with Article 5, Paragraph 2 hereof.

7. Effect of Termination by Purchase. Upon the purchase of one Partner's Partnership Interest pursuant to Article 9, Paragraph 5 or Article 8, Paragraph 1 above and in the event that only one Partner remains following such purchase, the Partnership shall be deemed terminated by way of a Termination by Purchase, and the one remaining Partner shall succeed to all of the properties, assets and liabilities of the Partnership, including without limitations, all rights to the Partnership's name and business operations and all rights and obligations of the Partnership pursuant to the RSA License Agreement and the Cylink License Agreement. Following such purchase, the remaining Partner shall indemnify, defend and hold the other Partner harmless with respect to any liabilities, debts and obligations of the Partnership, whether existing at the date of purchase or incurred after such date, except any such liability, debt, or obligation created as a result of the breach by the other Partner of this Agreement, the Joint Venture Agreement or any of the other Ancillary Agreements.

8. Distribution Of Licensed Rights. In the event of Termination By Dissolution pursuant to Article 6, Paragraph 6(b), or pursuant to Paragraph 6, herein, the Licensed Rights shall be distributed to the Partners as provided in the Cylink License Agreement and the RSA License Agreement. In addition, in the event of Termination By Dissolution under said Paragraphs, RSA will continue to receive 20% of all royalties received by CKC, its Affiliates or assignees from any sublicenses covered by the Stanford Agreement entered into after the effective date of dissolution shall be paid to RSA.

ARTICLE 10 - SIGNATURES

Except as may otherwise be agreed in writing between the Partners, any agreement, instrument, bill of sale or other document shall be executed on behalf of the Partnership by such persons as are designated by the Management Committee, and no other signature shall be permitted or required to bind the Partnership.

ARTICLE 11 - CONFIDENTIALITY

1. Each Partner acknowledges and agrees that certain information it receives from one or both of the other parties constitutes the confidential and proprietary trade secrets of the disclosing Partner, and that the receiving Partner's protection thereof is essential to this Agreement and a condition of the receiving Partner's use and possession thereof. Each Partner shall retain in strict confidence any and all such confidential information marked by the disclosing Partner as confidential (collectively "Confidential Information") and use such Confidential Information only as expressly authorized herein. A Partner will under no circumstances distribute or in any way disseminate Confidential Information to third parties without the prior written permission of the disclosing Partner.

2. Notwithstanding the above, the receiving Partner shall have no liability to the disclosing Partner with regard to any information which:

(a) was generally known and available in the public domain at the time it was disclosed or becomes generally known and available in the public domain through no fault of the receiving Partner;

(b) was known to the receiving Partner at the time of disclosure as shown by the files of the receiving Partner in existence at the time of disclosure;

(c) is disclosed with the prior written approval of the disclosing Partner;

(d) was independently developed by the receiving Partner without any use of Confidential Information, and by employees or other agents of the receiving Partner who have not been exposed to such Confidential Information;

(e) becomes known to the receiving Partner from a source other than the disclosing Partner without breach of this Agreement by the receiving Partner and otherwise not in violation of the disclosing Partner's rights; or

(f) is disclosed pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided, that the receiving Partner shall provide prompt, advance notice thereof to enable the disclosing Partner to seek a protective order or otherwise prevent such disclosure.

(3) Each Partner will enter into a confidentiality agreement with each employee who is given access to the Confidential Information of the other Partner which incorporates

the protections and restrictions substantially as set forth herein.

(4) Each Partner agrees to notify the other Partner in the event of any breach of its security under conditions in which it would appear that Confidential Information was prejudiced or exposed to loss. Each Partner shall, upon request of the disclosing Partner, take all other reasonable steps necessary to recover any compromised Confidential Information disclosed to or placed in its possession by virtue of this Agreement. The cost of taking such steps shall be borne solely by the receiving Partner.

(5) Each Partner acknowledges that any breach of any of its obligations under this Article 11 is likely to cause or threaten irreparable harm to the other Parties, and, accordingly, each Partner agrees that in such event the disclosing Partner shall be entitled to equitable relief to protect its interests, including but not limited to preliminary and permanent injunctive relief, as well as money damages.

ARTICLE 12 - MISCELLANEOUS

1. Arbitration. All disputes, controversies or differences arising out of or in relation to or in connection with this Agreement, which cannot be settled by discussion and mutual accord, shall be finally settled by arbitration. Each Partner shall be entitled to appoint one arbitrator, who shall not be an Affiliate, officer, director, employee, agent, vendor or contractor of that Partner. The two appointed arbitrators shall then appoint a third arbitrator, and the arbitration shall be conducted by the three arbitrators so chosen. All arbitrators so appointed shall be experienced in the business of licensing intellectual property rights, and the third arbitrator shall be a practicing attorney in said field. The arbitration shall be conducted in Santa Clara County, California. Demand for arbitration shall be made in writing and shall be served upon the Partner to whom the demand is addressed in the manner provided for the tender of notices in Article 12, Paragraph 2 hereof. If the Partner receiving the demand for arbitration does not appoint its arbitrator within 30 days after receiving such notice, the arbitrator appointed by the Partner demanding arbitration shall be further empowered to serve as the sole arbitrator with all of the rights, duties and powers granted hereunder without the necessity of a three person panel. The arbitrators are authorized to award any remedy, legal or equitable, as well as any interim relief as they deem appropriate in their discretion. Application may be made to any court having jurisdiction over the proceedings to assist the arbitrators in performing their arbitral duties, to confirm their award and to enforce any such award as a judgement of said court.

2. Notices and Other Communications. Every notice or other communications required or contemplated by this Agreement by either Partner shall be delivered in writing either by (i) personal delivery, or (ii) postage prepaid return receipt requested certified mail addressed to the Partner for whom intended at the address for such Partner specified above, or at such other address as the intended recipient previously shall have designated by written notice to the other Partner. Notice by certified mail shall be effective on the date it is officially recorded as delivered to the intended recipient by return receipt or equivalent, and in the absence of such record of delivery, the effective date shall be presumed to have been the fifth (5th) business day after it was deposited in the mail. All notices and other communication required or contemplated by this Agreement delivered in person shall be deemed to have been delivered to and received by the addressee and shall be effective on the date of personal delivery. Notice not given in writing shall be effective only if acknowledged in writing by a duly authorized representative of the Partner to whom it was given.

3. Counterparts. This Agreement may be executed in any number of counterparts, and each counterpart shall constitute an original instrument, but all such separate counterparts shall constitute only one and the same instrument.

4. Law to Govern. This validity, construction and enforceability of this Agreement shall be governed in all respects by the law of California applicable to agreements negotiated, executed and performed in California between California corporations, whether one or more of the parties shall now be or hereafter become a resident of another state or country.

5. No Waiver of Rights. All waivers hereunder must be made in writing, and failure at any time to require the other Partner's performance of any obligation under this Agreement shall not affect the right subsequently to require performance of that obligation. Any waiver of any breach of any provision of this Agreement shall not be construed as a waiver of any continuing or succeeding breach of such provision or a waiver or modification of the provision.

6. Attorneys' Fees. If either Partner hereto fails to perform any of its obligations under this Agreement, or if a dispute arises concerning the meaning or interpretation of any provision of this Agreement, the defaulting Partner or the Partner not prevailing in such dispute, as the case may be, shall pay any and all costs and expenses incurred by the other Partner in resolving such dispute or in enforcing or establishing its rights hereunder, whether by arbitration, litigation, negotiation by the parties or otherwise, including, without limitation, court costs, arbitration costs and actual attorneys' fees. In the event suit or arbitration is brought to enforce or interpret any part of this

Agreement, the prevailing Partner shall be the Partner which is entitled to recover its costs, whether or not the proceeding reaches a final judgment.

7. Severability. Whenever possible, each provision of this Agreement shall be interpreted in such manner as to be effective and valid under applicable law, but if any provision of this Agreement should be prohibited or invalid under applicable law, such provision shall be ineffective to the extent of such prohibition or invalidity without invalidating the remainder of such provision or the remaining provisions of this Agreement.

8. Subject Headings. The subject headings of the Articles and Sections of this Agreement are included for the purpose of convenience of reference only, and shall not affect the construction or interpretation of any of its provisions.

9. Further Assurances. The parties hereto shall each perform such acts, execute and deliver such instruments and documents, and do all such other things as may be reasonably necessary to accomplish the transactions contemplated in this Agreement.

10. Expenses. Except as otherwise agreed, the parties hereto shall each bear their own costs and expenses (including attorneys' fees) incurred in connection with the negotiation and preparation of this Agreement and consummation of the transactions contemplated hereby.

11. Omissions or Delays. No omission or delay on the part of any Partner hereto in requiring a due and punctual fulfillment by any other Partner hereto of the obligations of such other Partner hereunder shall be deemed to constitute a waiver by the omitting or delaying Partner of any of its rights to require such due and punctual fulfillment of any other obligations hereunder, whether similar or otherwise, or a waiver of any remedy it might have.

12. Entire Agreement; Amendments. The terms and conditions contained in this Agreement and in the various other agreements contemplated herein constitute the entire agreement between the parties hereto and supersede all previous communications, either oral or written, between the parties hereto with respect to the subject matter hereof, and no agreement or understanding varying or extending the same shall be binding upon any Partner hereto unless in writing signed by a duly authorized officer or representative thereof in which this Agreement is expressly referred to.

13. Assignment and Succession. This Agreement shall inure to the benefit of and be binding upon the parties hereto and their respective successors and assigns. Except as provided in Article

8, Paragraph 2, this Agreement shall not be assignable by any Partner except with the written consent of both of the other parties. In the event of any such assignment the transferor or assignor shall remain obligated to perform its own obligations and in addition shall be jointly and severally liable for the proper performance of the obligations of the transferee or assignee pursuant to this Agreement.

14. Adjustment of Basis. The Partnership shall, if either Partner so requests, elect pursuant to U.S. Internal Revenue Code Section 754, to adjust the basis of Partnership property under the circumstances and in the manner provided in U.S. Internal Revenue Code Sections 754 and 743. The Partners shall, in the event of such an election, take all necessary steps to effect the election.

15. Exculpation. Except in case of gross negligence or willful misconduct, the doing of any act or failure to do any act by either Partner, the effect of which may cause or result in loss or damage to the Partnership, if done pursuant to advice of legal counsel employed by the Partnership, or if done in good faith to promote the best interests of the Partnership, shall not subject such Partner to any liability to the other Partners or the Partnership.

16. Indemnification.

(a) General. The Partnership, its receiver or its trustee, shall indemnify and defend each Partner, their employees, agents, Affiliates, officers, directors, and assigns, against and hold them harmless from any and all losses, costs, damages, liabilities, claims and expenses arising out of the business of the Partnership (including, but not limited to, attorneys' fees and court costs, which shall be paid by the Partnership as incurred), which may be made or imposed upon such persons by reason of any (1) act performed for or on behalf of the Partnership or in furtherance of the Partnership business, (2) inaction on the part of such persons, or (3) liabilities arising under federal and state securities laws; so long as said conduct shall not constitute gross negligence or willful misconduct.

(b) Partnership Assets Must First be Used. All judgments against the Partnership and the Partners or their employees, agents, Affiliates, officers, directors and assigns wherein the Partners or such other persons or entities are entitled to indemnification, must first be satisfied from Partnership assets before the Partners or such other persons or entities are responsible for these obligations.

IN WITNESS WHEREOF, each Partner hereto has executed this Agreement on the date set forth opposite the name of each.

"CKC" CARO-KANN CORPORATION

By *Robert P. Long*
Title *President*

"RSA" RSA DATA SECURITY, INCORPORATED

By *R. James Bidza*
Title *President*

Exhibit B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

RSA DATA SECURITY, INC., and
MASSACHUSETTS INSTITUTE OF
TECHNOLOGY,

Plaintiffs,

v.

DIGITAL SIGNATURE, ROGER
SCHLAFLY and MICHAEL
MARKOWITZ,

Defendants.

Civil Action No.
87 C 9172

Judge Ilana D. Rovner

CONSENT JUDGMENT

The parties hereto, by their respective attorneys,
having appeared before the Court and consenting to the entry
of this decree;

IT IS HEREBY ORDERED, ADJUDGED AND DECREED:

Parties and Jurisdiction

1. Plaintiff RSA DATA SECURITY, INC. ("RSA Data") is a Delaware corporation having its principal place of business in the County of San Mateo, state of California.
2. Plaintiff MASSACHUSETTS INSTITUTE OF TECHNOLOGY ("MIT") is a Massachusetts corporation having its principal place of business in Cambridge, Massachusetts.
3. Defendant DIGITAL SIGNATURE ("Digital") is a partnership having its principal place of business and residing in the Northern District of Illinois.
4. Defendant MICHAEL MARKOWITZ ("Markowitz") is an individual and a general partner of defendant Digital.

5. Defendant ROGER SCHLAFLY ("Schlafly") is an individual and a general partner of defendant Digital.

6. The parties RSA Data and MIT are referred to herein as the "Plaintiffs."

7. The defendants Digital, Markowitz and Schlafly are referred to herein, individually and collectively, as the "Defendants."

8. This Court has jurisdiction over the parties hereto and the subject matter of this action. Venue is properly placed in the district and division of this Court.

Background

9. U.S. Patent No. 4,405,829 ("the '829 patent"), entitled CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD, issued on September 20, 1983. Plaintiff MIT is the assignee of all right, title and interest in the patent with the exception of a nonexclusive license held by the United States.

10. Plaintiff MIT granted to Plaintiff RSA Data an exclusive license under the patent, together with the right to sue infringers thereof on or about September 29, 1983. RSA Data has marketed, sold and licensed and continues to market, sell and license a cryptographic communications system and method that embodies the invention claimed in the '829 patent under the name "RSA Public Key Cryptosystem."

11. Defendants, from about December, 1983 to about July, 1987, sold a computer program system entitled

"CRYPT MASTER." More than one version of CRYPT MASTER was developed and marketed by Defendants. Further, several copies of CRYPT MASTER were given away by Defendants.

12. The CRYPT MASTER program, in all of its versions, was designed to encrypt data files stored on either floppy or hard disks. CRYPT MASTER, in all its versions, was an implementation of the RSA public key cryptosystem and the NBS Data Encryption Standard ("DES").

13. Defendants represent to this Court and to plaintiffs that approximately 100 copies of CRYPT MASTER were sold or given away by Defendants. Defendants further represent that the total dollar amount of the CRYPT MASTER sales by Defendants was about \$20,000. Defendants represent that several of the purchasers of a CRYPT MASTER program incorporated the program in products eventually sold to the government. Defendants further represent that no sales or transfer of CRYPT MASTER in any of its versions has occurred since July, 1987. Plaintiffs shall be permitted to make application to this Court for additional relief if any of Defendants' representations made herein are false. Damages for any additional past sales shall be at the royalty rate of 10%.

14. In its marketing of CRYPT MASTER, defendants have referred to the "RSA public key cryptosystem" as being implemented or used in CRYPT MASTER. This referred to the patented RSA Public Key Cryptosystem exclusively licensed to RSA Data.

15. On or about April 3, 1984, Defendant Schlafly received a letter from the President of Plaintiff RSA Data providing notice of the existence of the '829 patent.

16. Plaintiffs contend that Defendants' making, using and selling the CRYPT MASTER program infringes the '829 patent. Defendants do not admit that making, using and selling the CRYPT MASTER program infringes the '829 patent.

17. Defendants do not admit the validity of the '829 patent.

Relief Granted

18. Defendants are hereby enjoined from making, using and selling any products using or implementing the public key cryptosystem described and claimed in U.S. Patent No. 4,405,829 and from otherwise infringing, inducing infringement or contributing to the infringement of U.S. Patent No. 4,405,829 except under prior written approval of RSA Data or under license from RSA Data or under license of the United States Government.

19. Defendants are hereby enjoined from making, using or selling the Defendants' CRYPT MASTER program in any of its versions, including CRYPT MASTER/8, CRYPT MASTER/16 and CRYPT MASTER/24, for the life of U.S. Patent No. 4,405,829 except under prior written approval from RSA Data or under license from RSA Data or under license of the United States Government. Notwithstanding the other provisions of paragraphs 18 and 19, Defendants shall be permitted

to manufacture and design products in accordance with the license of the United States Government.

20. Defendants are hereby enjoined from advertising or commercially using the designation "RSA" in connection with any cryptosystem, encryption or decryption system or algorithm. The Defendants may state, in connection with each transaction or sale under the United States Government's license to U.S. Patent No. 4,405,829 that its CRYPT MASTER program or equivalent program employs the cryptosystem or algorithm described and claimed in U.S. Patent No. 4,405,829 invented by Messrs. Rivest, Shamir and Adleman.

21. Defendants shall make no sale, delivery or transfer of any product that uses or implements the public key cryptosystem described and claimed in U.S. Patent No. 4,405,829 or infringes, induces infringement of or contributes to the infringement of U.S. Patent No. 4,405,829, including Defendants' CRYPT MASTER program, to the United States Government or other U.S. Government authorized recipient without Defendants first receiving a written request ("Written Request") from the United States Government that it is exercising its rights under its license to U.S. Patent No. 4,405,829, and in such event Defendants shall maintain information ("Information") for each such sale, transfer or delivery, including a copy of the Government's Written Request, the date of the Request and the product(s) or item(s) sold, transferred or delivered and the name and address of the receiving entity. The

Information shall be made available for quarterly inspection by an independent auditor that RSA Data may designate ("Designee") on behalf of RSA Data. RSA Data initially designates the firm of Laventhol & Horwath to make inspection of the Information. Defendants shall also provide to RSA's Designee quarterly, beginning on January 1, 1989, a written statement setting forth the number of products sold, transferred and delivered under the Government's license during the applicable time period and if no products have been sold, transferred or delivered, the written statement shall so state. Every sale, delivery or transfer by any of Defendants of any product under the United States Government's license to U.S. Patent No. 4,405,829 shall be accompanied by a written notice, displayed prominently on the product, that "the making, using and selling of this product is limited, in accordance with the U.S. Government's license to U.S. Patent No. 4,405,829 and any use, sale, or reproduction by persons not specifically licensed is prohibited." The "Information" reviewed by the Independent Auditor shall be kept confidential and shall be used only to determine compliance of and for enforcement of this Decree and shall not be disclosed to RSA Data or MIT. In the event that the auditor concludes in its view that there has been noncompliance by Defendants, then the "Information" relating to such noncompliance may be disclosed to RSA Data and MIT or its representatives.

22. Defendants agree to and shall pay to Plaintiffs promptly upon entry of this Decree by the Court the

amount of one-thousand, eight hundred dollars (\$1,800.00) in settlement of any claims concerning use of U.S. Patent No. 4,405,829 prior to the date of this Decree.

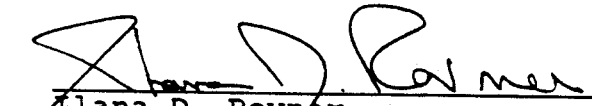
23. This Court makes no finding as to validity or invalidity of the '829 patent.

24. The Complaint, and all Counterclaims of the parties are hereby dismissed with prejudice.

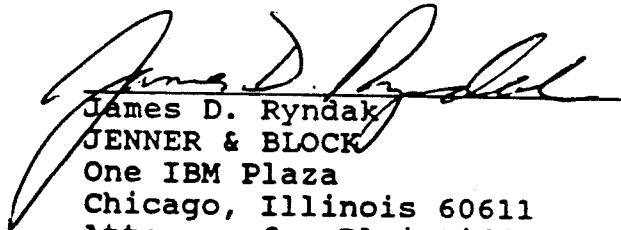
25. Each party shall pay its own respective attorney's fees and costs.

26. This Court shall retain jurisdiction of this cause to enforce the terms of this Decree, upon application of any party hereto.

ENTERED AS OF NOVEMBER 15, 1988.


Ilana D. Rovner
United States District
Court Judge

APPROVED AS TO FORM
AND FOR ENTRY


James D. Ryndak
JENNER & BLOCK
One IBM Plaza
Chicago, Illinois 60611
Attorney for Plaintiffs

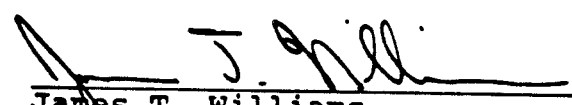

James T. Williams
NEUMAN, WILLIAMS, ANDERSON
& OLSON
77 West Washington Street
Chicago, Illinois 60602
Attorney for Defendants

Exhibit D

PKP

PUBLIC KEY PARTNERS

January 12, 1994

By Federal Express

AT&T Federal Systems Advanced Technologies
Guilford Center, Room 3D24
185 & Mt. Hope Church Road
P.O. Box 25000
Greensboro, North Carolina 27420

Attention: Chief Financial Officer

Re: Patent License Agreement Dated July 1, 1992

Dear Sirs:

We refer to the referenced license agreement and the enclosed press releases announcing ATT's "Secret Agent" program and software modules licensed by AT&T from Information Security Corporation of Deerfield, New Jersey ("ISC"). We hereby protest such actions by AT&T and ISC based on the following:

Breach Of the Consent Judgement

ISC is the successor in interest to a partnership known as Digital Signature. We enclose a copy of the Consent Judgment dated November 15, 1988, in which ISC's principals were

... enjoined from making, using and selling any products using or implementing the public key cryptosystem described and claimed in U.S. Patent No. 4,405,829 and from otherwise infringing, inducing infringement or contributing to the infringement of U.S. Patent No. 4,405,829 except under prior written approval of RSA Data or under license from RSA Data

We also enclose a copy of ISC's letter dated September 14, 1993, to the undersigned in response to our inquiries concerning ISC's adherence to the terms of this injunction. You will note their advice that ISC "... has not sold any RSA programs in the commercial sector" and that it "...has suspended commercial sales ..." of DSA programs.

Please advise when ISC entered into its agreement with AT&T and whether ISC informed AT&T of this injunction. In any event, to the extent any of AT&T's products are tainted by ISC's violation of this injunction, we hereby demand that AT&T cease their further distribution and sale.

AT&T Federal Systems Advanced Technologies
Chief Financial Officer
Patent License Agreement Dated July 1, 1992
January 12, 1994


Practice of The Digital Signature Algorithm

We note from the enclosed announcements AT&T's interest in practicing the Digital Signature Algorithm ("DSA"). While AT&T's existing license does not authorize this practice, PKP hereby offers to modify AT&T's license to include the practice of the DSA in accordance with PKP's pending cross

license with the Federal Government as described in the Federal Register notice dated June 8, 1993. While PKP is naturally disappointed that AT&T failed to raise this issue with PKP in a more orderly way, PKP would be pleased to negotiate an equitable adjustment of the existing license to incorporate this additional technology.

In view of the seriousness of this matter, we look forward to hearing from you at your earliest convenience.

Very truly yours,



Robert B. Fougner, Esq.
Director of Licensing

RBF/sg

cc. By Fax: 908-949-0292

Gregory C. Ranieri, Senior Attorney

Mr. D. James Bidzos

Exhibit E



LETTERS TO THE EDITORS

Psychics and Weapons

In "Bang! You're Alive" ["Science and the Citizen," *SCIENTIFIC AMERICAN*, April], on research into nonlethal weaponry, writer John Horgan addressed my interest in the paranormal. I am a member of the Society for Scientific Exploration and do endorse the rigorous scientific study of various anomalous phenomena. My personal and professional interests in such topics have included involvement in studies by the National Research Council and other governmental scientific bodies.

Those interests, however, have nothing to do with my development of nonlethal technologies and concepts. They do not in any way constitute part of my work at Los Alamos National Laboratory. Belief systems, whether religious, political or otherwise, should not be reported in articles on scientific topics. Similarly, they have no bearing on the validity of nonlethal weapons. The urgent need to provide new options to military and law enforcement agencies should be self-evident.

Your article has done a disservice to our nation. Innuendo and obfuscation don't belong in science.

JOHN B. ALEXANDER
Los Alamos National Laboratory
Los Alamos, N.M.

Horgan replies:

The government pays Alexander to oversee a multimillion-dollar research program. His "interest" in alien abductions and paranormal phenomena, about which most scientists are deeply skeptical, raises questions about his judgment and is therefore a legitimate part of the story.

Privileged Communications

In "Wire Pirates" [*SCIENTIFIC AMERICAN*, March], Paul Wallich writes: "Within the U.S., patent rights to public-key encryption are jealously guarded by RSA Data Security.... Although software employing public-key algorithms has been widely published, most people outside the government cannot use it without risking an infringement suit."

This is wrong and is a myth perpetuated by those who don't bother to check their facts. RSA Data Security provides

necessary patent licenses for public-key technology at reasonable rates and actively promotes the widespread use of public-key technology. Licensees include IBM, AT&T, Motorola, Microsoft and other companies, large and small. Moreover, the technology is available royalty free for noncommercial and educational use. More than three million installed software packages utilize RSA; it is far and away the most widely used public-key cryptographic technique.

Thus, although RSA is patented, it is generally an easy matter to obtain a relevant patent license. Only those who are ignorant of the patent or disregard it run any actual risk.

JIM BIDZOS
President
RSA Data Security, Inc.
Redwood City, Calif.

Wallich replies:

As Bidzos knows, the widely published public-key software to which that passage refers is PGP, a free program available worldwide to tens of millions of computer users. PGP makes unlicensed use of algorithms for which RSA holds U.S. patents. (Viacrypt, a small company that had previously purchased a general license from RSA, distributes a commercial version of PGP.) Although RSA makes some of its software available royalty free for noncommercial use within the U.S., until recently the company blocked efforts to incorporate that software into the free version of PGP. On May 9 the Massachusetts Institute of Technology announced a U.S.-only, noncommercial version of PGP that uses RSA-licensed software.

Congress and Altruism

In the middle of Natalie S. Glance and Bernardo A. Huberman's "The Dynamics of Social Dilemmas" [*SCIENTIFIC AMERICAN*, March], I started thinking about term limits and the effect they would have on parliamentary compromise. If "cooperation is most likely in small groups with lengthy interactions," then term limits on Congress and other legislatures would make our already fractious politics even more vitriolic.

DAVID OLSON
Princeton, N.J.

I believe the authors' conclusions are seriously flawed, in part because they do not fully take into account the effects of irrational behavior and altruism. Many human decisions are based not on perceived good to the individual but on perceived good to others, even at the expense of the individual decision maker. Most religions actively espouse such behavior, and most individuals incorporate some degree of altruism into their decisions.

Failure to incorporate irrationality, altruism and other relevant cultural biases into these sorts of computer models of human behavior renders those models grossly inaccurate and highly misleading.

STEPHEN C. FOX
New York City

Glance and Huberman reply:

When altruism is pervasive, cooperation is easily achieved. When irrationality reigns, anything can happen. But our results will still hold when the influence of altruism is not dominant in a social group. The need all over the world to enforce taxation is an example of how dilemmas persist in all countries.

Altruism and piety confer benefits on individuals that are not quantifiable and perhaps not even acknowledged at a conscious level but are benefits nonetheless. Religious beliefs allow a person to have an infinite horizon for future interactions, because he or she expects benefits to continue eternally. Within this framework, a religious individual is behaving rationally.

Letters selected for publication may be edited for length and clarity. Unsolicited manuscripts and correspondence will not be returned or acknowledged unless accompanied by a stamped, self-addressed envelope.

ERRATUM

The special issue of *Scientific American* entitled *Ancient Cities*, published in April, misstated the chronology of the pre-Columbian city of Teotihuacán, in what is now Mexico. The city was founded in the first century B.C. and declined to insignificance after A.D. 750, centuries before the period of Aztec dominance in the 14th through 16th centuries A.D.

Exhibit F

April 4, 1994

David DeVita, Esq.
c/o
Information Security Corporation
1141 lake Cook Road, Suite D
Deerfield, IL 60015

Re: Public Key License

Dear David:

I refer to your letters dated February 10 and March 18.

Unfortunately, the renewed vacillation by the Government has postponed resolution of licensing for DSS and the other PKP patents. In this regard, I enclose a copy of my letter dated March 28, 1994, to the ANSI and IEEE Committees.

As for Information Security, the matter is further complicated by ISC's recent relationship with AT&T, as discussed in the enclosed copy of my letter dated January 12, 1994 to AT&T. In view of this apparent breach of the November 15, 1988, Consent Judgement, I am not in a position at present to discuss licensing of RSA for ISC.

Very truly yours,



Robert B. Fougner

RBF/sg
cc. Mr. D. James Bidzos

Exhibit G

Mr. Robert Fougner
Director of Licensing
Public Key Partners
310 North Mary Avenue
Sunnyvale, CA 94086

April 4, 1994

Dear Mr. Fougner,

I have heard that you have been telling people that I have breached a consent judgment or that I have infringed patents. This is a serious matter.

In order to protect my rights, reputation, and business relationships, I demand that you immediately:

- (1) Acknowledge this letter, and confirm or deny the allegation.
- (2) Cease and desist any such actions.
- (3) Provide me with a complete list of persons and businesses that you have contacted, and copies of letters that you have sent regarding me.
- (4) Send written retractions to each party, with copies going to me.

Sincerely,

Roger Schlafly
Digital Signature
PO Box 1680
Soquel, CA 95073

Exhibit H

April 18, 1994

PUBLIC KEY PARTNERS

Mr. Roger Schlafly
Digital Signature
PO Box 1680
Soquel, Ca. 95073

Re: Public Key Patents

Dear Mr. Schlafly:

I acknowledge receipt of your letter of April 4.

The Massachusetts Institute of Technology and the Board of Trustees of the Leland Stanford Junior University have granted Public Key Partners ("PKP") exclusive sublicensing rights to the following patents registered in the United States, and all of their corresponding foreign patents:

- Cryptographic Apparatus and Method ("Hellman-Diffie")..... No. 4,200,770
- Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582
- Cryptographic Communications System and Method ("RSA") No. 4,405,829
- Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414

In addition, PKP has received by assignment all rights to the following invention:

- Method For Identifying Subscribers And For Generating And Verifying Electronic Signatures In A Data Exchange System ("Schnorr") No. 4,995,082

In the action filed in the United States District Court for the Northern District of California (CV-93-20450) captioned Roger Schlafly vs. National Institute Of Standards And Technology you admitted marketing a commercial application of DSA technology. The practice of the DSA is described in the Hellman-Diffie, Hellman-Merkle and Schnorr patents, and your use of the DSA for commercial application constitutes an unlicensed use of said patents.

Unfortunately, your letter is defectively vague, in that you merely state you "have heard" that PKP has made some general allegations to unspecified people. Before I can respond, please advise the following:

Mr. Roger Schlafly
Digital Signature
Re: Public Key Patents
April 18, 1994

- (i) to whom were these statements allegedly made?
- (ii) which patents are you referring to?
- (iii) when and how were these statements allegedly made?
- (iv) who, in turn, made these allegations about our conduct?

In any event, based on your own admission, it appears you have infringed on numerous patents. As for the existence of a consent judgement, I refer to the Consent Judgement entered on November 18, 1988 in the United States District Court in the action RSA Data Security Inc. and the Massachusetts Institute of Technology vs. Digital Signature, Roger Schlafly and Michael Markowitz (Civ. No. 87 C. 9172). In order to determine whether you are in breach of this Consent Judgement, please advise:

- (i) what is the nature of your prior and existing business relationship, if any, with Information Security Corporation?
- (ii) what is the nature of your current use of the technology described in the RSA patent?

I look forward to your response.

Truly yours,

RBF/sg
cc. Mr. D. James Bidzos

Exhibit I

Mr. Robert Fougner
Director of Licensing
Public Key Partners
310 North Mary Avenue
Sunnyvale, CA 94086

April 21, 1994

Dear Mr. Fougner,

I received your letter of April 18, 1994. Neither your name nor signature was on it, but I assume that it was written by you. It did not address the demands in my April 4 letter.

My letter was not "defectively vague". To be precise, I object to you telling ANYONE that I infringed ANY patents at ANY time. Any such statement by you is a tort. How I might learn of such statements is irrelevant.

Your assertion that the practice of the DSA is described in your patents is nonsense. The DSA was devised subsequent to those patents. If your intent was to say that practice of the DSA infringes those patents, I am not aware of any legal argument as why that would be the case. If you wish to make such an argument, please explain which claims are infringed by the DSA, and how each element of those claims corresponds to an element of the DSA.

For the record, I have not admitted to infringing any patents. The precise nature of my business relationships is not your concern. Any use that I might be making of RSA technology complies with applicable laws, and that is all you need to know.

I repeat my demand that you comply with my April 4 letter.

Sincerely,

Roger Schlafly
PO Box 1680
Soquel, CA 95073

Exhibit J

Mr. Robert Fougner
Director of Licensing
Public Key Partners
310 North Mary Avenue
Sunnyvale, CA 94088

Feb. 6, 1994

Dear Mr. Fougner,

I have recently been informed that PKP has agreed to abide by ANSI's patent policy, in connection with certain standards which are in progress. Under this policy, PKP must make patent licenses "available to applicants under reasonable terms and conditions that are demonstrably free of any unfair discrimination".

I am interested in obtaining a license to the Stanford and MIT patents that you control.

I would greatly appreciate it if you would send me a copy of your licensing policy. I would like to know exactly the terms under which such a license would be available to me.

If I don't hear from you in two weeks, then I will assume that no such policy exists.

Sincerely,

Roger Schlafly
PO Box 1680
Soquel, CA 95073

Mr. Robert Fougner
Director of Licensing
Public Key Partners
310 North Mary Avenue
Sunnyvale, CA 94086

April 11, 1994

Dear Mr. Fougner,

I received your letter of April 4, 1994, but it did not address my request. When I talked to you in 1990, you told me that you did not have a standard patent licensing policy, but that each agreement is negotiated on a case-by-case basis. I was hoping that maybe you had adopted a policy since then.

Yes, I am on the IEEE P1363 committee. If you tell me your licensing policy, I can report that information to the committee.

Sincerely,

Roger Schlafly
PO Box 1680
Soquel, CA 95073

April 4, 1994

Mr. Roger Schlafly
Soquel Numerics
PO Box 1680
Soquel, Ca. 95073

Re: Public Key License

Dear Mr. Schlafly:

Thank you for your letter of February 6. I regret being unable to reply earlier due to the press of travel commitments and other business.

I enclose for your ease of reference a copy of my letter to you dated September 24, 1990, concerning PKP's licensing policy. I also enclose a copy of my recent letter dated March 28, 1994, to the ANSI and IEEE standards committees. I believe you are a member of the IEEE committee.

Very truly yours,



RBF/sg
enc.
cc. Mr. D. James Bidzos

September 24, 1990


Mr. Roger Schlafly
Soquel Numerics
PO Box 1680
Soquel, Ca. 95073

Re: Public Key License

Dear Mr. Schlafly:

Thank you for your letters of September 11 and 21. Our standard license terms include a \$25,000 signing fee and a minimum annual royalty payment of \$10,000 per year. If you are still interested in obtaining a license please give me a call to schedule a meeting.

Sincerely,



Robert B. Fougner
Director of Licensing

Mr Robert Fougner
Director of Licensing
Public Key Partners
310 North Mary Avenue
Sunnyvale, CA 94086

May 26, 1994

Dear Mr Fougner,

I have not received answers to my letters of April 11 and 21.

I am on the IEEE P1363 committee, as you know, and we are considering technologies which might be free of patent claims. In particular, we are looking at ElGamal and elliptic curve public key encryption.

I am told that you control these patents:

Diffie-Hellman	4,200,770
Hellman-Merkle	4,218,582
RSA	4,405,829
Hellman-Pohlig	4,424,414
Schnorr	4,995,082

I have an analysis which asserts that the ElGamal and elliptic curve public key encryption methods do not infringe any of these patents. Are you disputing this? If so, please explain which claims of which patents are infringed. Also is the infringement literal, and how do the elements of the claim(s) correspond to those encryption methods?

I hope you are aware that making invalid patent claims in order to monopolize a market may violate antitrust laws, and that Federal Circuit court rulings have limited the scope of patent claims.

I am sure that you have considered these questions, so I'll expect a prompt answer. If I don't hear from you in two weeks, I will conclude that there is no infringement, and I will inform others that these technologies are in the public domain as far as PKP is concerned.

Sincerely,

Roger Schlafly
PO Box 1680
Soquel, CA 95073

August 25, 1993

By Fax: 708-405-0506
David DeVita, Esq.
c/o
Information Security Corporation
1141 lake Cook Road, Suite D
Deerfield, IL 60015

Re: Public Key License

Dear David:

I refer to your letter of August 19 which I have circulated among my principals for a response to your inquiry concerning RSA.

In order to expedite PKP's response please confirm as soon as possible by return fax that, to date, ISC has not sold any public key products (including DSA) to non-government parties.

Thank you for your early reply.

Sincerely,



Bob Fougner

RBF/sg

CALLER B-E 2/2.17

November 7, 1991

Mr. Thomas J. Venn, President
Information Security Corporation
320 North Michigan Ave., Suite 2100
Chicago, ILL 60601

Re: Public Key

Dear Mr. Venn:

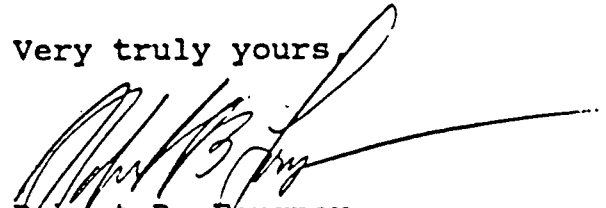
I refer to your letters of March 18, April 15 and July 7.

The use of El Gamal is covered by the Hellman-Merkel patent.

Our standard license fee is \$25,000 plus a minimum annual royalty of \$10,000. A copy of the royalty schedule is enclosed. Please let me know whether you are interested in receiving our license agreement.

I look forward to hearing from you.

Very truly yours,



Robert B. Fougner
Director of Licensing

enc.

TELEPHONE
(415) 595-8782

RSA DATA SECURITY, INC.
DIGITAL SIGNATURES FOR DATA ASSURANCE
10 TWIN DOLPHIN DRIVE
REDWOOD CITY, CALIFORNIA 94065

June 3, 1986

Mr. Roger Schlafly, Partner
Digital Signature
5453 S. Woodlawn Avenue
Chicago, IL 60615

Dear Mr. Schlafly:

Enclosed is a copy of our current patent license agreement for your review. As you are aware, we are obligated to MIT to license all users of the RSA Public Key Cryptosystem. I'm certain that you would agree that it is in everyone's best interests to obtain a license to use and sell any patented technology.

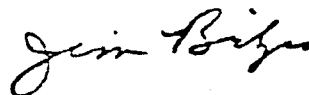
We understand that it is possible that revenues obtained from the sale of RSA based products may not financially justify the purchase of a license. Recognizing this, we are willing to negotiate payment terms that would allow both of us to accommodate our needs.

It is important for both of us to initiate the necessary steps to address and resolve this issue. If you do not feel that there is sufficient value in RSA technology and do not market or plan to discontinue marketing such products, please make us aware of the situation.

I feel that a prudent next step would be a written response to us indicating your plans regarding RSA based products, and how we could begin discussing mutually agreeable licensing terms.

I look forward to hearing from you.

Sincerely,



Jim Bidzos
Vice President

cc: Ralph Bennett
Prof. Ron Fivest

TELEPHONE
(415) 595-8782

RSA DATA SECURITY, INC.
DIGITAL SIGNATURES FOR DATA ASSURANCE
11 TWIN DOLPHIN DRIVE
REDWOOD CITY, CALIFORNIA 94065

September 16, 1986

Mr. Roger Schlafly, Partner
Digital Signature
5453 S. Woodlawn
Chicago, IL 60615

Dear Mr. Schlafly:

We are in receipt of your letter of September 11, 1986. I will address all of your questions regarding a patent license for use of the RSA algorithm.

The "field of use" defines the application of the RSA algorithm to your particular product. It is determined for each individual licensee. Typical examples are "encryption key management and distribution for digital link encryptors" or "message authentication/author identification for electronic files". The \$25,000 license fee is for the license itself; new products with their respective field of use and royalty rates may be added without taking another license.

Regarding the MIT agreement with RSA: please note that we represent in our agreement that we are fully empowered to enter into such agreement by MIT. You should contact Mr. Jake Maslow, Esq., at MIT to satisfy yourself on this issue or if there are further questions. He can be reached at (617)253-6696.

You note that references have been made to "RSA modules" as well as "Technical information" and "Know-How". These references were to software products and/or design consulting services that may be purchased from RSA Data Security, Inc. We ourselves are licensed to make, use and sell products utilizing the RSA algorithm. The purchase of such products or services is optional and available to anyone. Such issues have no relation to your acquiring a patent license to make, use or sell products using the RSA algorithm.

We do not feel the term "digital signature" by itself can be trademarked. Since you state you were advised by your legal counsel on this, I suggest you have them contact Mr. Hodges, our counsel, at (415)494-7622, who advises us in this matter. This is, nonetheless, a separate issue from the patent license.

I believe this letter addresses all of your concerns and questions. I look forward to your prompt reply as to the next step in your acquiring a license from us.

Sincerely,

Jim Bidzos
Jim Bidzos
Vice President

cc: David P. Hodges, Esq.

Exhibit K

PUBLIC KEY PART

March 15, 1991

RECEIVED

Ms. Cindy Fuller, Secretariat
American Bankers' Association
1120 Connecticut Ave. N.W.
Washington D.C. 20036

MAR 21 1991

ABA STANDARDS DEPT.

Re: X9 Financial Services

Dear Ms. Fuller:

I refer to Rev. Greenlee's letter of February 20, 1991, concerning the terms and availability of licenses to practice public key, specifically any art covered by the Hellman or RSA patents.

PKP has previously announced its policy concerning the availability of licenses on a non-discriminatory basis to all parties. Since its inception, PKP has not denied a license to any party.

In order to preserve the element of equal treatment, PKP offers a standard license for the manufacture, sale and use of products on university licensing terms, similar to those offered by both Stanford University and MIT. The license costs \$25,000 with an annual minimum royalty of \$10,000 for all four patents. The annual minimum can be adjusted depending on the specific patents licensed.

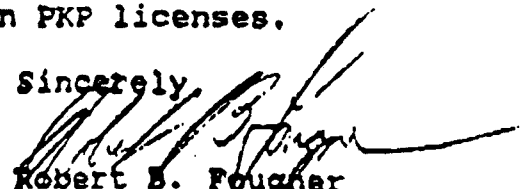
Royalties are calculated on a sliding scale in accordance with the sale price of the end products. A copy of this schedule is enclosed.

This scale was created to meet the concerns of vendors that a flat percentage rate, regardless of end product price, discriminated against the higher value systems. In other words, the declining scale of royalties corresponds to the diminishing comparative value of the patented technology to the overall product value.

I would point out that the royalty rates, at 1% or less, are very modest when compared with typical patent licenses which range from 3%-5%.

Thank you for your interest in PKP licenses.

Sincerely,



Robert B. Fougner
Director of Licensing

Exhibit O

November 20, 1991

Federal Express
National Institute of Standards and Technology
Computer Sciences Laboratory
Technology Building, Room B-154
Gaithersburg, MD 20899

Attention: Director

Re: Proposed FIPS For DSS

Dear Sirs:

We represent the patent holders of the following Public Key patents issued in the United States, and all of their corresponding foreign patents:

- Cryptographic Apparatus and Method ("Diffie-Hellman")..... No. 4,200,770
- Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582
- Cryptographic Communications System and Method ("RSA") No. 4,405,829
- Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414

These patents represent the collective work product of the undisputed inventors of Public Key and are the dominant patents covering all known methods of practicing this art, including the variations collectively known as El Gamal on which the proposed DSS is derived.

We have previously gone on record as offering to license these patents for use in digital signatures under reasonable terms and conditions on a non-discriminatory basis (See Our letter of April 20, 1990 to Dr. Dennis K. Branstad of NIST). As evidence of this policy, the majority of U.S. computer manufacturers and software vendors has already licensed either the patents or technology created by the patents' licensees (See Letter of D. James Bidzos, President of RSA Data Security Inc., dated September 20, 1991).

By making this offer we invited NIST to engage in straightforward commercial discussions of the patent issues. NIST responded by ignoring our invitation and continues to sidestep the issue. In his statement to the Subcommittee on Technology and Competitiveness on June 27, 1991, Deputy Director Krammer announced, without the benefit of any prior discussion with the

National Institute of Standards and Technology
Computer Sciences Laboratory
FIPS Proposed DSS
November 20, 1991

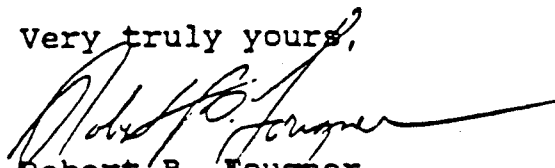
dominant patent holders, that NIST intended to make its El Gamal DSS " ... available world-wide on a royalty free basis". Yet the very existence of the inventors' patents clearly contradicts NIST's ability to offer anyone a "royalty free" license to DSS. (See Our letter of August 1, 1991, to NIST). Such bald statements reflect either NIST's incomprehension of the patent issues, or a deliberate effort to undermine the inventors' rights.

In his reply to our concerns, counsel for NIST contends that the inventors' patents "...do not apply to DSS" (See Letter of John H. Raubitschek, Esq. dated August 16, 1991). We flatly disagree. (See Letter of Dr. David H. Newman, Esq. dated November 19, 1991, enclosed). Moreover, NIST itself acknowledges that "Implementation of ... this standard may be covered by U.S. and foreign patents. (emphasis added)." (See NIST's Proposed DSS "Patents"). Recognizing the existence of patent issues, the visibility of these patents, and their widespread acceptance, why has NIST chosen such a confrontational path?

Consider the consequences. NIST is charged with responsibility for paving the way to industry's rapid adoption of standards to enhance its security. Instead, NIST's reticence to acknowledge the patent holders' rights is misleading at best, and most certainly an invitation to litigate. What, then, will be industry's enthusiasm for this long overdue standard? In this light, how can NIST fairly state that it has properly fulfilled its mandate?

There are those that theorize NIST's actions betray their principals' reluctance to see any Public Key standards come to fruition. NIST's seemingly belligerent attitude toward Public Key's inventors and patent holders only adds credence to such theories.

Very truly yours,



Robert B. Fougner
Director of Licensing

RBf/pe
enc.

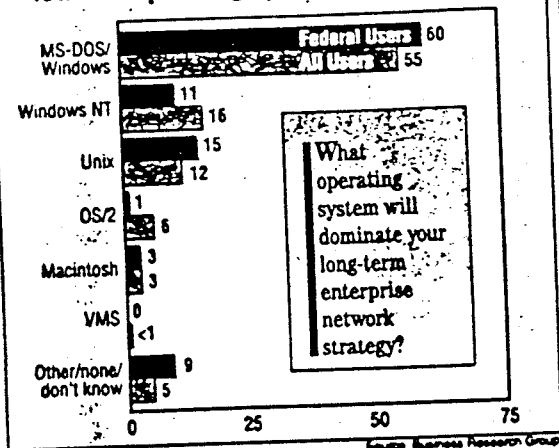
Exhibit P

GOVERNMENT COMPUTER NEWS

THE NATIONAL NEWSPAPER OF GOVERNMENT COMPUTING ■ A CAHNERS PUBLICATION ■ VOLUME 13, NUMBER 11 ■ MAY 30, 1994

Enterprise networks
in the federal government
Special report follows Page 39

Federal networks build on low-end operating systems for long term



What operating system will dominate your long-term enterprise network strategy?

More so than their private-sector counterparts, federal agencies plan to stick with their existing PC and Unix operating systems as they build enterprise architectures.

Study confirms fed preference for TCP/IP, not mandatory OSI

BY SAM MASUD
GCN Staff

Federal agencies are more likely than any other sector of the economy to use the TCP/IP protocol, independent researchers reported this month.

For both LANs and interdepart-

mental backbones, the government is less likely to use Open Systems Interconnection protocols even though OSI is mandatory for federal agencies, according to the new study by Business Research Group.

"The study confirms what has
see TCP/IP Page 73

FTS 2000 pioneer Mike Corrigan catches buy-out fever, leaves GSA

BY SUSAN M. MENKE AND
TIM MINAHAN
GCN Staff

Michael L. Corrigan, one of the original leaders of the FTS 2000 team, plans to take an early-out offer and leave his post as senior telecommunications official in the General Services Administration's IRM Service by year's end.

"I haven't made up my mind where I'm going next," Corrigan told GCN, "but somewhere in telecom. I'm young enough and have enough energy to do some things you can't necessarily do in government."

Corrigan, a career government employee who went to GSA from the Defense Department, was on
see BUY-OUTS Page 74

VA hit for not meeting milestones

Despite modernization, processing slows from 181 days to 215

BY JAMES M. SMITH
GCN Staff

The multimillion-dollar Veterans Benefits Administration systems modernization effort is again the focus of intense congressional and oversight review.

According to General Services Administration officials, VBA has not kept its promises to speed up processing of veterans benefits claims and, in fact, processing now takes longer than in the past.

The problems have touched off a high-level review of the Veterans Affairs Department's delegation of procurement authority for the VBA project. In a May 24 memo, Joe

Thompson, commissioner of GSA's IRM Service, asked Mark Catlett, assistant secretary of VA for finance and IRM, to respond to GSA's concerns.

Sources said GSA has asked for VBA records, reviews and personnel information.

In a telephone interview, Catlett acknowledged that "we are a little behind" on meeting milestones VBA had agreed to achieve. Last year, in response to concerns that big spending on new systems might not improve the agency's performance, VA officials agreed to link further spending to performance measurements.

He said VA officials would meet

soon with GSA representatives to explain the delays. "We're feeling good about our claims processing at this point," Catlett said.

VBA has spent \$42 million on new hardware and software under a
see VBA Page 73

NIST approves DSS despite threat of a patent lawsuit

BY VANESSA JO GRIMM
GCN Staff

The Commerce Department has taken its biggest risk yet with the Digital Signature Standard, approving it as a Federal Information Processing Standard in the face of threats of a patent lawsuit.

DSS becomes mandatory Dec. 1 for agencies using digital signature applications. The new standard, FIPS 186, can be used royalty-free by anyone. National Institute of Standards and Technology spokeswoman Anne Enright Shepherd said.

Free use of the standard is the issue in a continuing battle between NIST, on the one side, and Public

Key Partners of Sunnyvale, Calif., and RSA Data Security Inc. of Redwood City, Calif., on the other. PKP and RSA insist that the algorithm NIST uses in DSS infringes on their public-key encryption patents.

Scientists at NIST and the National Security Agency designed DSS as a means of verifying the senders and contents of electronic messages. The NIST Computer Security Laboratory built the standard around the public-key-based Digital Signature Algorithm (DSA).

Last summer, NIST and PKP had agreed that government agencies would use DSS free but private-sector users would have to pay the company a royalty fee (GCN, June
see STANDARD Page 73

Informix takes leap into data warehousing

BY SEAN GALLAGHER
GCN Staff

SAN FRANCISCO—Informix Software Inc. broke into the rarefied domain of high-end data warehousing at last week's DB/Expo '94 here.

Steven Sommer, Informix vice president of marketing, detailed the data warehousing plans for Informix-OnLine Dynamic Server jointly with Jim Ashbrook, president of Prism Solutions Inc., a Sun-
see WAREHOUSE Page 72

INSIDE



S.W. Hall Jr. describes the quality drive at Energy

GCN Snapshot
Page 16

Tips on selecting a 32-bit operating system

Buyers Guide
Page 61

Our reviewer rates 4 Windows comm packages

Product Reviews
Page 33

Is the pen dead? Once-hot pen computing needs a killer app

BY CYNTHIA MORGAN
GCN Staff

ATLANTA—The rumors of pen computing's death may have been greatly exaggerated. Or maybe not.

"Pretty much everyone who will be using it already uses it,"

Steven Andler, mobile business strategies marketing director for AST Research Inc., said at Spring Comdex last week.

AST, which acquired pen leader Grid Systems Corp. last year, discontinued all but the smallest of the GridPad pen syst-
see PEN Page 72

SECOND CLASS MAIL

NIST holds ground on DSS in face of threats to file suit

STANDARD from Page 1

21, 1993, Page 1). Because the government sponsored the research that resulted in the DSA, agencies are exempt from licensing fees.

But in the face of mounting pressure to find a completely free signature standard for both public and private users, NIST officials backed out of that agreement.

"It's still our position that DSS infringes our patent, and we've put NIST on notice," said James Bidzos, president of both RSA and PKP. PKP holds rights to public-key patents on behalf of RSA, Stanford University, and Massachusetts Institute of Technology and German professor Claus P. Schnorr.

But NIST now disagrees. In a justification paper prepared for Commerce Secretary Ronald Brown, NIST said, "Based on an analysis of existing patents, NIST believes the DSA does not infringe on any known patents."

NIST Deputy Director Raymond Kammer, who in February said the agency would search for a royalty-free DSS, declined to explain why the agency revised its stance on the patent

rights issue and decided to proceed with DSS approval. The NIST spokeswoman said Kammer would not comment because discussions between PKP and NIST are continuing.

Up In the air

NIST now claims to hold patent rights to DSA. The agency reported to Brown that it filed a successful claim with the Patent and Trademark Office. "The patents that are claimed to be infringed were directly or indirectly referenced in the DSA patent application," NIST's report said.

Nonetheless, Bidzos said, "nothing is settled. We're very surprised NIST would do this."

Bidzos said legal action is an option for PKP. He suggested that suing someone in the private sector might be easier than suing a government agency. "We have sued companies in the past and won, including TRW Inc. over a DSS-like algorithm," Bidzos said.

It still is unlikely the government will see widespread use of digital signature applica-

tions for several years, said F. Lynn McNulty, associate director for computer security at NIST's Computer Systems Laboratory.

Implementing DSS "will be fairly difficult in some respects because it's going to take a commitment to security and integrity that many agencies have not had before," McNulty said. The use of digital signatures also requires some technical savvy, he said.

Additionally, there are some gray policy areas the administration must resolve. Specifically, the Office of Management and Budget must establish a policy for handling signature certificates that validate a user's electronic

signature, McNulty said. And there's the issue of cost. "The agencies will have to expend some resources up front," he said. The government also needs a policy that sets out when use of electronic signatures becomes too expensive and paper would be cheaper, McNulty added.

"It's going to be years before you really see it in large government applications where the government interacts electronically with large populations of the public," McNulty said. Initially, agencies will use electronic signatures for internal applications—time cards, payroll and the like, he said.

Hill, GSA again review VBA project

VBA from Page 1

contract awarded to Federal Data Corp. of Bethesda, Md., in December 1992. Calllett said more than half of the 57 regional VBA claims processing centers have gotten new equipment.

More backlogs

But the most recent review noted that claims processing times and backlogs had increased, a source said.

It took VBA an average of 181 days to process a new application for benefits early in 1992. Although VBA had agreed to cut processing time for those claims to 176 days this year, the processing now takes as long as 215 days, sources familiar with the project said.

Based on the latest figures from VBA and the GSA concerns, Rep. John Conyers Jr. (D-Mich.) has asked the General Accounting Office to review the modernization effort

again. In a letter to GAO, he questioned whether VBA was living up to the performance terms outlined in its June 24, 1993, agreement.

Conyers, chairman of the House Government Operations Committee, also plans to call a hearing on the program soon, committee staff members said.

At the time of the agreement, VA Secretary Jesse Brown said VBA "will make more productive use of our resources and will serve as an example of the administration's success in changing the way government operates."

Last fall, GAO even lauded VBA for the improvements it had made in the modernization program.

The Federal Data Corp. contract represents the first of three phases of the modernization program.

Calllett said Stage II was on schedule for contract award late this summer.

TCP/IP fed user protocol of choice

TCP/IP from Page 1

long been whispered behind closed doors," said Gregory P. Cline, program director of BRG's network integration and management service. "The war is over between commercially successful TCP/IP and the government-mandated OSI Profile, with GOSIP suffering a crushing defeat."

BRG estimated that 38 percent of the traffic on federal LANs is TCP/IP, compared with 35 percent in the manufacturing sector, 26 percent in the trade sector, 24 percent in the health-care industry and 15 percent in the financial sector.

Management Information Protocol is likely to be maintained," the study said. "But it is unclear at this point just what SNMP Version 2's ultimate impact will be."

The Federal Internetworking Requirements Panel of senior IRM officials has recommended scrapping the GOSIP mandate and opening the door to other networking schemes [GCN, Jan. 24, Page 1]. No decision has been made on the controversial recommendation.

Exhibit Q

March 28, 1994

Ms. Cindy Fuller, Secretariat
American Bankers' Association
1120 Connecticut Ave. N.W.
Washington D.C. 20036

Dr. Burt Kaliski, Chairman
The IEEE Computer Society
100 Marine Parkway
Redwood City, CA 94056

Re: X9 Committee On Financial Services
P1363 RSA/Diffie-Hellman Working Group

Dear Ms. Fuller and Dr. Kaliski:

I refer to both the IEEE's and the ABA's letters of March 9 and March 18, respectively, which request clarification of Public Key Partners' licensing policies.

In its settlement proposal published in the June 8, 1993, Federal Register, NIST sought to regulate PKP's patent licensing policies concerning the Digital Signature Algorithm for practicing the Digital Signature Standard. Despite PKP's assurances attached to NIST's proposal, and additional concessions made by PKP during the ensuing negotiations, the Government withdrew its settlement proposal on February 4, 1994. It is our understanding that the Government now prefers an arrangement with PKP in which the DSA can be practiced on a royalty free basis, both for Government and private use, worldwide. However, as of this date, an agreement with the Government has not yet been achieved.

In light of these changing circumstances, and the uncertainty of the outcome, it would be inappropriate at this time to renew any previous assurances concerning PKP's licensing policies for DSS. Dependent as they are on a final agreement, if any, with the Government, re-formulation of PKP's commercial licensing policies must be left temporarily in abeyance.

In the meantime, the Government continues to abide by its understanding with PKP to defer promulgation of the Federal DSS until the matter is resolved. Similarly, and in keeping with both ANSI's and IEEE's patent policies, we must ask that promulgation of any commercial standards concerning the practice of the DSS be postponed until PKP can harmonize its licensing policies with the Government's latest position. Failing such postponement, continuation of standards efforts respecting the DSS at this time will conflict with both organizations express


Ms. Cindy Fuller, Secretariat
X9 Committee On Financial Services
American Bankers' Association

Dr. Burt Kaliski, Chairman
The IEEE Computer Society
March 28, 1994

policies respecting the availability and uniformity of the
requisite patent licenses.

We would be pleased to speak with your committees
concerning this matter and, in the meantime, would
appreciate confirmation of your concurrence with this request.

Sincerely,


Robert B. Fougner
Director of Licensing

RBF/sg

cc. Mr. D. James Bidzos

Exhibit R

April 20, 1990

Registered Mail
National Institute of Standards
225 Technology
Gaithersburg, Maryland 20879

Attention: Dr. Dennis K. Branstad

Re: Public Key Standards and Licenses

Dear Sirs:

The Massachusetts Institute of Technology and the Board of Trustees of the Leland Stanford Junior University have recently granted Public Key Partners exclusive sublicensing rights to the following patents registered in the United States, and all of their corresponding foreign patents:

- Cryptographic Apparatus and Method ("Diffie-Hellman")..... No. 4,200,770
- Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582
- Cryptographic Communications System and Method ("RSA") No. 4,405,829
- Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414

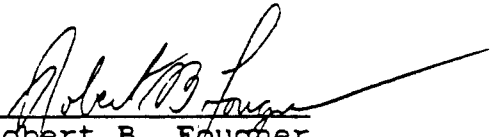
These patents cover all known methods of practicing the art of Public Key, including the variations collectively known as El Gamal.

Due to the broad acceptance of RSA digital signatures throughout the international community, Public Key Partners strongly endorses its incorporation in a digital signature standard. We assure the interested parties listed below that Public Key Partners will comply with all of the policies of ANSI and the IEEE concerning the availability of licenses to practice this art. Specifically, in support of any RSA signature standard which may be adopted, Public Key Partners hereby gives its assurance that licenses to practice RSA signatures will be available under reasonable terms and conditions on a non-discriminatory basis.

We take this opportunity to thank all of those concerned for their collective efforts in making this technology readily available for commercial implementation.

National Institute of Standards
Attention: Dr. Dennis K. Branstad
April 20, 1990

Very truly yours,
Public Key Partners

By: 
Robert B. Foucher
Director of Licensing

RBF\alr

cc:

Dr. John W. Lyons, Director NIST
Mr. Raymond G. Kammer, Deputy Director NIST
Mr. James Burrows, Director of the National Computer Systems
Laboratory, NIST
Ms. Lynn McNulty, Associate Director NIST
Mr. Miles Smid, NIST
The Honorable Robert Mosbacher, Secretary of Commerce
The Honorable Nicholas F. Brady, Secretary of the Treasury
Mr. Marty Ferris, Department of the Treasury
Mr. James H. Miller, Director, Office Automation Support and
Technology, Office of the Secretary of Defense
William Rockwell, Esq., General Counsel, ANSI
Mr. Jean Paul Emard, Secretariat X3
Ms. Cindy Fuller, Secretariat X9
Mr. Robert Kaminski, Chairman, X9
Mr. Joel Bloom, Chairman, X9A3
Mr. Richard Yen, Chairman, X9E9
Secretariat: ASC X12, Data Interchange Standards Association
Mr. Glenn R. J. Mules, Co-Chairman, X12F/TG4
Dr. Horton L. Sorkin, Co-Chairman, X12F/TG4
Ms. Helen Wood, President, IEEE
Mr. Robert Pritchard, IEEE Standards Office
Ms. Lisa D. Granoien, Assistant Director for Standards, IEEE
Computer Society
Mr. Stan Ames, Chairman of the Standards Committee, IEEE Security
and Privacy Technical Committee,
Dr. Jon Graff, Chairman, Committee for Standards of Public Key
Algorithms, Chairman
Mr. Jim Randall, Co-Chairman, 802.10 (SILS) Working Group
Mr. Russell Housley, Co-Chairman 802.10 (SILS) Working Group
Dr. Harold Podell, House Science Committee
Mr. Tim Bolin, Chairman, OSI Implementors Workshop
Mr. Jim Galvin, Chairman, OSI Implementors Workshop Security SIG
Mr. Paul Lambert, Chairman, OSI Implementors Workshop Key
Management SIG

Exhibit S

March 13, 1991

By Fax: 312-368-0326
Information Security Corporation
320 North Michigan Ave., Suite 2100
Chicago, ILL 60601

Attention: Mr. Thomas J. Venn, President

Re: Public Key

Dear Sirs:

We have noted with interest your statements concerning your product Crypt Master and in particular your use of Public Key technology.

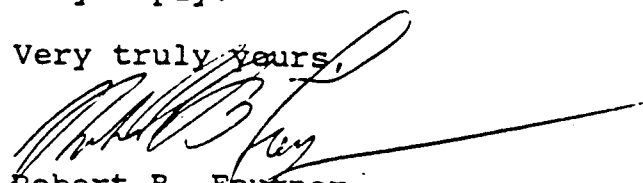
The Massachusetts Institute of Technology and the Board of Trustees of the Leland Stanford Junior University have recently granted Public Key Partners ("PKP") exclusive sublicensing rights to the following patents registered in the United States, and all of their corresponding foreign patents:

- Cryptographic Apparatus and Method ("Hellman-Diffie")..... No. 4,200,770
- Public Key Cryptographic Apparatus and Method ("Hellman-Merkle")..... No. 4,218,582
- Cryptographic Communications System and Method ("RSA") No. 4,405,829
- Exponential Cryptographic Apparatus and Method ("Hellman-Pohlig")..... No. 4,424,414

These patents cover all known methods of practicing the art of Public Key, including the implementation known as El Gamal.

According to our records, Information Security does not have a license to practice Public Key technology. Please contact the undersigned as soon as conveniently possible to discuss the availability of a license to manufacture and sell your Public Key product. We look forward to your early reply.

Very truly yours,



Robert B. Fougner
Director of Licensing

Exhibit T

Multiuser cryptographic techniques*

by WHITFIELD DIFFIE and MARTIN E. HELLMAN
Stanford University
Stanford, California

ABSTRACT

This paper deals with new problems which arise in the application of cryptography to computer communication systems with large numbers of users. Foremost among these is the key distribution problem. We suggest two techniques for dealing with this problem. The first employs current technology and requires subversion of several separate key distribution nodes to compromise the system's security. Its disadvantage is a high overhead for single message connections. The second technique is still in the conceptual phase, but promises to eliminate completely the need for a secure key distribution channel, by making the sender's keying information public. It is also shown how such a public key cryptosystem would allow the development of an authentication system which generates an unforgeable, message dependent digital signature.

INTRODUCTION

In a computer network with a large number of users, cryptography is often essential for protecting stored or transmitted data. While this application closely resembles the age old use of cryptography to protect military and diplomatic communications, there are several important differences which require new protocols and new types of cryptosystems. This paper addresses the multiuser aspect of computer networks and presents ways to preserve privacy of communication despite the large number of user connections which are possible.

In a system with n users there are $n^2 - n$ pairs who may wish to hold private conversations. The straightforward way to achieve this is to give each pair of users a key in common which they share with no one else. Each user will then have $n-1$ keys, one for communicating with each other user. Unfortunately, the cost of distributing these keys is prohibitive. A new user must send keys to all other users. Unfortunately, the network cannot be used for this purpose, and an external

secure channel is required. This procedure is comparable to requiring each new telephone subscriber to send a registered letter to everyone else in the phonebook.

Military communications suffer less from this problem for several reasons. Among these are the limitations imposed by the chain of command and the fact that stations change allegiance infrequently. In a computer network designed for business communication, on the other hand, users will regard each other as friends on one matter and as opponents on another. Firms A and B may cooperate on one venture in competition with C, while simultaneously, A and C compete with B on a different endeavor. A must therefore use different keys for communicating with B and C.

One approach to this problem is to assume that the users trust the network. Each user remembers only one key which is used to communicate with a local node. From there the message is relayed from node to node, each of which decrypts it, then reencrypts it in a different key for the next leg of its journey. This process is known as link encryption.¹ When the message reaches the network node closest to its destination, it is sent on to the addressee encrypted in a key shared only by the addressee and that node.

Although this technique requires each user to remember only one key, it has the disadvantage that a message is compromised if any one of the nodes in its path is subverted. In this paper we examine two other ways of allowing secure communication between any pair of users without assuming the integrity of all nodes in the network and without requiring the users to distribute or store large numbers of keys.

The first technique requires no new technology, but imposes a complex initial connection protocol. This is the subject of the second section of this paper. We call the second technique public key cryptography, since most of the secrecy traditionally required for the keys has been removed. This is discussed in section three and represents a radical departure from past cryptographic practices. While it requires further work before it becomes implementable its simplicity of operation makes it extremely attractive. If a suc-

* This work was supported by the National Science Foundation under NSF Grant ENG 10173.

successful implementation can be developed it should find wide use in both military and civilian applications.

The fourth section shows how public key cryptography can be used to provide a time and message dependent digital signature which cannot be forged even when past signatures have been seen. This is an example of the general problem of authentication discussed in greater detail in Reference 2, which provides a more general perspective in which public key cryptography can be viewed.

A PROTECTIVE PROTOCOL

As indicated earlier, a message protected by link encryption will be compromised if any node in the path it follows from the sender to the receiver is subverted. In this section we describe a protocol which guarantees to protect the message unless a large number of nodes are compromised. While many variations are possible, the basic technique is as follows.

A small number m of the network's nodes will function as "key distribution nodes." Each user has m keys, one for communicating with each of these m nodes. These keys vary from user to user, so while each user must remember only m keys, each of the key distribution nodes remembers n , one for each user of the net. When users A and B wish to establish a secure connection they contact the m key distribution nodes and receive one randomly chosen key from each. These keys are sent in encrypted form using the keys which the users share with the respective nodes. Upon receiving these keys, the conversants each compute the exclusive or of the m keys received to obtain a single key which is then used to secure a private conversation. None of the nodes involved can violate this privacy individually. Only if all m nodes are compromised will the security of this connection fail.

It might be objected that any key distribution node acting alone can prevent all communication by mischievously sending out different keys to each of the parties, thus bringing network operations to a halt. The users, however, can easily protect themselves against this threat. If communication using the composite key fails, its use as a key is abandoned, and the components are exchanged one by one, in clear, for comparison. If any key fails to agree, the node which issued it is blacklisted. Finally, on conclusion of this process, the users repeat the request for keys to the nodes which passed the previous test.

Alternatively, the component keys can be compared by the use of one way functions^{2,3,5} without ever being transmitted in clear. Loosely speaking, a function f is called a one-way function if it is easy to compute in the forward direction, but given any output, it is computationally infeasible to find an input which produces it. In referring to a task as computationally infeasible, we have in mind that it cannot be done in

fewer than a finite but astronomical number of operations, say 2^{100} . For practical purposes, this is equivalent to being incomputable. As shown in Reference 2, a one way function can easily be obtained from a secure cryptosystem.

If communication fails using the composite key, the users send the images of the individual keys under a public one-way function. If the image received does not agree with that computed by applying f to the key, the node which issued it is guilty of compromise. Since the valid keys have not been publicly revealed in this process, there is no need to request new ones from the uncompromised nodes. Instead the invalid ones are omitted and the remainder xored.

To sum up, this technique requires each user to remember m keys and each key distribution node to remember n keys. Unless all m key distribution nodes are subverted, any two users can establish a private link through use of a set-up protocol usually requiring $2m$ exchanges (more are required if a key distribution node has been subverted). The next section describes a concept which eliminates much of this overhead and does not require the user to trust any node. This new concept, if successfully implemented, will make the technique described above obsolete.

PUBLIC KEY CRYPTOGRAPHY

In this section we propose that it is possible to eliminate most of the secrecy surrounding the key used in a communication, and yet to preserve the secrecy of the communication. This is accomplished by giving each user a pair of keys E and D . E is an enciphering key and is public information. D is the corresponding deciphering key, and while this must be kept secret, it need never be communicated, eliminating the need for a secure key distribution channel. Although D is determined by E , it is infeasible to compute D from E .

For reasons of security, generation of this E - D pair is best done at the user's terminal which is assumed to have some computational power. The user then keeps the deciphering key D secret but makes the enciphering key E public by placing it in a central file along with his name and address. Anyone can then encrypt a message and send it to the user, but only the intended receiver can decipher it. Public key cryptosystems can therefore be regarded as multiple access ciphers.

By regularly checking the file of enciphering keys the user can guard against any attempt to alter it surreptitiously. Any such mischief is reported and settled by other authentication means, such as personal appearance.

The crucial feature of a public key system is that it is relatively easy to generate an E - D pair, preferably automatically through a publicly available transformation from a random bit string to E - D , and yet it is computationally infeasible to compute D from E .

At present we have neither a proof that public key systems exist, nor a demonstration system. We hope to have a demonstration E-D pair in the near future, and expect that if the demonstration pair successfully resists attack then we will be able to design an algorithm for automatically generating E-D pairs of a similar kind. In the meantime, the following reasoning is given to help dispel any doubts the reader may have.

A suggestive example is to let the cryptogram, represented as a binary n -vector c equal $E m$; where m is the message also represented as a binary n -vector, and E is an arbitrary n -by- n invertible matrix. Letting $D = E^{-1}$ we have $m = D c$. Thus both enciphering and deciphering are easily accomplished with about n^2 operations. Calculation of D from E , however, involves a matrix inversion which is a harder problem. And it is at least conceptually simpler to obtain an arbitrary pair of inverse matrices than it is to invert a given matrix. Start with the identity matrix I and do elementary row and column operations to obtain an arbitrary invertible matrix E . Then starting with I do the inverses of these same elementary operations in reverse order, to obtain $D = E^{-1}$. The sequence of elementary operations could easily be generated from a random bit string.

Unfortunately, matrix inversion takes only about n^3 operations even without knowledge of the sequence of elementary operations. The ratio of "cryptanalytic" time (i.e., computing D from E) to enciphering or deciphering time is thus at most n . To obtain ratios of 10^6 or greater would thus require enormous block sizes. Also, it does not appear that knowledge of the elementary operations used to obtain E from I greatly reduces the time for computing D . And, since there is no round-off error in binary arithmetic numerical stability is of no consequence in the matrix inversion. In spite of its lack of practical utility, this matrix oriented example is still useful for clarifying the relationships necessary in a public key system.

A more practical direction uses the observation that we are really seeking a pair of easily computed inverse algorithms E and D , but that D must be hard to infer from E . This is not as impossible as it may sound. Anyone who has tried to determine what operation is accomplished by someone else's machine language program knows that E itself (i.e., what E does) can be hard to infer from E (i.e., a listing of E). If the program were to be made purposefully confusing through addition of unneeded variables, statements and outputs, then determining an inverse algorithm could be made very difficult indeed. Of course, E must be complicated enough to prevent its identification from input-output pairs.

Another idea appears more promising. Suppose we start with a schematic of a 100 bit input, 100 bit output circuit which merely is a set of 100 wires implementing the identity mapping. Select 4 points in the circuit at random, break these wires, and insert AND,

OR and NOT gates which implement a randomly chosen 4 bit to 4 bit invertible mapping (a 4 bit S box in Feistel's notation). Then repeat this insertion operation approximately 100 times to obtain an enciphering circuit E . Knowing the sequence of operations which led to the final E circuit allows one to easily design an inverse circuit D . If however the gates are now randomly moved around on the schematic of E to hide their associations into S boxes, an opponent would have great difficulty in reconstructing the simple description of E in terms of S boxes, and therefore would have great difficulty in constructing a simple version of D . His task could be further complicated by using reduction techniques (e.g. Carnaugh maps) or expansion techniques (e.g. $\sim(AB) = \sim A$ or $\sim B$, or expressing a logical variable in terms of previous variables), and by adding additional, unneeded S boxes and outputs.

For ease of exposition, we have described the implementation of a specific key in hardware. In practice, a special purpose simulator is obviously of most interest. The hardware description is also valuable in exemplifying a generally useful idea. To build a good public key cryptosystem one needs easily inverted elementary building blocks and a general framework for describing the concatenation of these elementary blocks. Here the elementary building blocks are S boxes and the general framework is the schematic diagram. The general framework must also hide the sequence of elementary building blocks so that no one other than the designer can easily implement the sequence of inverse elementary operations. Examination will show that the matrix example had a similar structure, except there the general class of transformations obtainable was too small.

While the above arguments only provide plausibility as opposed to proof, we hope they will stimulate additional work on this promising area of research.

PUBLIC KEY AUTHENTICATION

The purpose of a cryptographic system is to prevent the unauthorized extraction of information from a public (i.e., insecure) channel. The dual problem of authentication is to prevent unauthorized injection of messages into a public channel.

In conventional paper oriented business transactions, signatures provide a generally accepted level of authentication. As electronic communication replaces mail service the need for a digital signature will be strongly felt.

Various types of authentication are now possible,² but the development of public key cryptosystems would allow an entirely new dimension.

Currently, most message authentication consists of appending an authenticator pattern, known only to the transmitter and intended receiver, to each message

and encrypting the combination. This protects against an eavesdropper being able to forge new, properly authenticated messages unless he has also stolen the key being used. There is no protection against such an eavesdropping thief or against the threat of dispute. That is, the transmitter may transmit a properly authenticated message, later deny this action, and falsely blame the receiver for taking unauthorized action. Or, conversely, the receiver may take unauthorized action, forge a message to itself and then falsely blame the transmitter for these actions. For example, a dishonest stockbroker may try to cover up unauthorized buying and selling for personal gain by forging orders from clients. Or a client may disclaim an order, actually authorized by him, but which is later seen to cause a loss. We will introduce concepts which would allow the receiver to easily verify the authenticity of a message, but which prevent him from generating apparently authenticated messages, thereby protecting against both the threat of eavesdropping thieves and the threat of dispute. Note that these techniques thus provide stronger protection than signatures, voiceprints, etc. which can be forged once seen and are not message dependent.

To obtain an unforgeable digital signature from a public key cryptosystem, the protocol would be as follows: Assume user A wishes to send a message M to user B. The transformed message $C = E_b D_a(M)$ is sent, where E_b represents the transformation effected by use of B's public enciphering key and D_a represents the transformation effected by use of A's secret deciphering key. Upon receipt of C , user B operates first with his secret operation D_b and then with the public operation E_a thereby obtaining $E_a D_b(C) = E_a D_b E_b D_a(M) = M$. No one else can extract M because of the need to know D_b . By saving the intermediate result $D_b(C) = D_a(M)$ user B (and only user B) can prove that he received the specific message M from user A. There must be some structure to the message (e.g., it could include a date and time field) to prevent injection of random bit patterns for C , with the hope that the resultant decoded "message", $E_a D_b(C)$, might cause random mischief such as deletion of files.

Note that since there is no need for a secure channel for distribution of authentication information, we have a public key authentication system. This system protects against, "eavesdropping thieves" and against a dispute as to whether or not an action taken by the receiver was authorized by the transmitter. Similarly, a public key cryptosystem can be used to protect

against the other type of dispute in which the transmitter A claims to have issued an order which was not carried out by the receiver B. The transmitter requests that the receiver B send $E_a D_b(M)$ as a receipt for the message M . By operating on this receipt with his secret operation D_a , the transmitter obtains $D_b(M)$, which could only have been generated by the receiver B. Only user A can generate this receipt since it requires knowledge of D_a .

While the above discussion centered on message authentication it also applies to user authentication. The implicit message becomes "I am user X and the time is T." Inclusion of the time field prevents an eavesdropper from using old authentication signals to pose as someone else. For reasons noted in Reference 2, such a system deserves to be called a one-way IFF system.

We thus see that public key cryptosystems developed for ensuring the privacy of communications, could also be used to ensure their authenticity. They could therefore be used to fill the need for a digital equivalent of a signature. This need is currently a major barrier to the use of electronic mail for business communications, and provides additional motivation for study of public key cryptosystems.

ACKNOWLEDGMENT

The authors wish to thank Leslie Lamport of Massachusetts Computer Associates for several valuable discussions. In particular, the technique described in Section 2 was discovered during one of these conversations.

REFERENCES

1. Baran, Paul, *On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations*, Santa Monica, CA: The Rand Corporation August 1964, (RM-3765-PR).
2. Diffie, Whitfield and Martin E. Hellman, forthcoming paper to be submitted to the *IEEE Transactions on Information Theory*.
3. Evans, Arthur, Jr., William Kantrowitz and Edwin Weiss, "A User Authentication System not Requiring Secrecy in the Computer," *Communications of the ACM*, Vol. 17 No. 8, August 1974, pp. 437-442.
4. Feistel, Horst, "Cryptography and Computer Privacy," *Scientific American*, Vol. 228, No. 5, May 1973, pp. 15-23.
5. Purdy, George B., "A High Security Log-in Procedure," *Communications of the ACM*, Vol. 17, No. 8, August 1974, pp. 442-445.

Exhibit U

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23-25, 1975 and the IEEE International Symposium on Information Theory in Rönneby, Sweden, June 21-24, 1976.

W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.

M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D . Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver's public enciphering key and decipheres the messages he receives using his own secret deciphering key.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of a different form.

A second problem, amenable to cryptographic solution, which stands in the way of replacing contemporary busi-

ness communication is guaranteed legal evidence present in every contract. This paper discusses a message but which even the messages be viewed authentic.

Section digital, message out there. problem. how any a one-way

Section cryptographically difficult p

At the s have given spring, inf have begun problems

The sea themes of all proposed nineteen t vented, an theoretica put on a fi mation th keys and applicatio

In contr resides in of discover This prob complexit plines whi problems.

possible to of systems this possib

Before p terminolog section.

II

Cryptog for solving authentica of informa

ness communications by teleprocessing systems is authentication. In current business, the validity of contracts is guaranteed by signatures. A signed contract serves as legal evidence of an agreement which the holder can present in court if necessary. The use of signatures, however, requires the transmission and storage of written contracts. In order to have a purely digital replacement for this paper instrument, each user must be able to produce a message whose authenticity can be checked by anyone, but which could not have been produced by anyone else, even the recipient. Since only one person can originate messages but many people can receive messages, this can be viewed as a broadcast cipher. Current electronic authentication techniques cannot meet this need.

Section IV discusses the problem of providing a true, digital, message dependent signature. For reasons brought out there, we refer to this as the one-way authentication problem. Some partial solutions are given, and it is shown how any public key cryptosystem can be transformed into a one-way authentication system.

Section V will consider the interrelation of various cryptographic problems and introduce the even more difficult problem of trap doors.

At the same time that communications and computation have given rise to new cryptographic problems, their offspring, information theory, and the theory of computation have begun to supply tools for the solution of important problems in classical cryptography.

The search for unbreakable codes is one of the oldest themes of cryptographic research, but until this century all proposed systems have ultimately been broken. In the nineteen twenties, however, the "one time pad" was invented, and shown to be unbreakable [2, pp. 398-400]. The theoretical basis underlying this and related systems was put on a firm foundation a quarter century later by information theory [3]. One time pads require extremely long keys and are therefore prohibitively expensive in most applications.

In contrast, the security of most cryptographic systems resides in the computational difficulty to the cryptanalyst of discovering the plaintext without knowledge of the key. This problem falls within the domains of computational complexity and analysis of algorithms, two recent disciplines which study the difficulty of solving computational problems. Using the results of these theories, it may be possible to extend proofs of security to more useful classes of systems in the foreseeable future. Section VI explores this possibility.

Before proceeding to newer developments, we introduce terminology and define threat environments in the next section.

II. CONVENTIONAL CRYPTOGRAPHY

Cryptography is the study of "mathematical" systems for solving two kinds of security problems: privacy and authentication. A privacy system prevents the extraction of information by unauthorized parties from messages

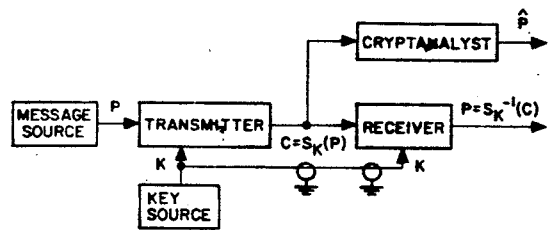


Fig. 1. Flow of information in conventional cryptographic system.

transmitted over a public channel, thus assuring the sender of a message that it is being read only by the intended recipient. An authentication system prevents the unauthorized injection of messages into a public channel, assuring the receiver of a message of the legitimacy of its sender.

A channel is considered public if its security is inadequate for the needs of its users. A channel such as a telephone line may therefore be considered private by some users and public by others. Any channel may be threatened with eavesdropping or injection or both, depending on its use. In telephone communication, the threat of injection is paramount, since the called party cannot determine which phone is calling. Eavesdropping, which requires the use of a wiretap, is technically more difficult and legally hazardous. In radio, by comparison, the situation is reversed. Eavesdropping is passive and involves no legal hazard, while injection exposes the illegitimate transmitter to discovery and prosecution.

Having divided our problems into those of privacy and authentication we will sometimes further subdivide authentication into message authentication, which is the problem defined above, and user authentication, in which the only task of the system is to verify that an individual is who he claims to be. For example, the identity of an individual who presents a credit card must be verified, but there is no message which he wishes to transmit. In spite of this apparent absence of a message in user authentication, the two problems are largely equivalent. In user authentication, there is an implicit message "I AM USER X," while message authentication is just verification of the identity of the party sending the message. Differences in the threat environments and other aspects of these two subproblems, however, sometimes make it convenient to distinguish between them.

Fig. 1 illustrates the flow of information in a conventional cryptographic system used for privacy of communications. There are three parties: a transmitter, a receiver, and an eavesdropper. The transmitter generates a plaintext or unenciphered message P to be communicated over an insecure channel to the legitimate receiver. In order to prevent the eavesdropper from learning P , the transmitter operates on P with an invertible transformation S_K to produce the ciphertext or cryptogram $C = S_K(P)$. The key K is transmitted only to the legitimate receiver via a secure channel, indicated by a shielded path in Fig. 1. Since the legitimate receiver knows K , he can decipher C by operating with S_K^{-1} to obtain $S_K^{-1}(C) = S_K^{-1}(S_K(P)) = P$, the original plaintext message. The secure channel cannot

be used to transmit P itself for reasons of capacity or delay. For example, the secure channel might be a weekly courier and the insecure channel a telephone line.

A *cryptographic system* is a single parameter family $\{S_K\}_{K \in \{K\}}$ of invertible transformations

$$S_K: \{P\} \rightarrow \{C\} \quad (1)$$

from a space $\{P\}$ of plaintext messages to a space $\{C\}$ of ciphertext messages. The parameter K is called the key and is selected from a finite set $\{K\}$ called the keyspace. If the message spaces $\{P\}$ and $\{C\}$ are equal, we will denote them both by $\{M\}$. When discussing individual cryptographic transformations S_K , we will sometimes omit mention of the system and merely refer to the transformation K .

The goal in designing the cryptosystem $\{S_K\}$ is to make the enciphering and deciphering operations inexpensive, but to ensure that any successful cryptanalytic operation is too complex to be economical. There are two approaches to this problem. A system which is secure due to the computational cost of cryptanalysis, but which would succumb to an attack with unlimited computation, is called *computationally secure*; while a system which can resist any cryptanalytic attack, no matter how much computation is allowed, is called *unconditionally secure*. Unconditionally secure systems are discussed in [3] and [4] and belong to that portion of information theory, called the Shannon theory, which is concerned with optimal performance obtainable with unlimited computation.

Unconditional security results from the existence of multiple meaningful solutions to a cryptogram. For example, the simple substitution cryptogram XMD resulting from English text can represent the plaintext messages: now, and, the, etc. A computationally secure cryptogram, in contrast, contains sufficient information to uniquely determine the plaintext and the key. Its security resides solely in the cost of computing them.

The only unconditionally secure system in common use is the *one time pad*, in which the plaintext is combined with a randomly chosen key of the same length. While such a system is provably secure, the large amount of key required makes it impractical for most applications. Except as otherwise noted, this paper deals with computationally secure systems since these are more generally applicable. When we talk about the need to develop provably secure cryptosystems we exclude those, such as the one time pad, which are unwieldy to use. Rather, we have in mind systems using only a few hundred bits of key and implementable in either a small amount of digital hardware or a few hundred lines of software.

We will call a task *computationally infeasible* if its cost as measured by either the amount of memory used or the runtime is finite but impossibly large.

Much as error correcting codes are divided into convolutional and block codes, cryptographic systems can be divided into two broad classes: *stream ciphers* and *block ciphers*. Stream ciphers process the plaintext in small chunks (bits or characters), usually producing a pseudo-random sequence of bits which is added modulo 2 to the

bits of the plaintext. Block ciphers act in a purely combinatorial fashion on large blocks of text, in such a way that a small change in the input block produces a major change in the resulting output. This paper deals primarily with block ciphers, because this *error propagation* property is valuable in many authentication applications.

In an authentication system, cryptography is used to guarantee the authenticity of the message to the receiver. Not only must a meddler be prevented from injecting totally new, authentic looking messages into a channel, but he must be prevented from creating apparently authentic messages by combining, or merely repeating, old messages which he has copied in the past. A cryptographic system intended to guarantee privacy will not, in general, prevent this latter form of mischief.

To guarantee the authenticity of a message, information is added which is a function not only of the message and a secret key, but of the date and time as well; for example, by attaching the date and time to each message and encrypting the entire sequence. This assures that only someone who possesses the key can generate a message which, when decrypted, will contain the proper date and time. Care must be taken, however, to use a system in which small changes in the ciphertext result in large changes in the deciphered plaintext. This intentional error propagation ensures that if the deliberate injection of noise on the channel changes a message such as "erase file 7" into a different message such as "erase file 8," it will also corrupt the authentication information. The message will then be rejected as inauthentic.

The first step in assessing the adequacy of cryptographic systems is to classify the threats to which they are to be subjected. The following threats may occur to cryptographic systems employed for either privacy or authentication.

A *ciphertext only attack* is a cryptanalytic attack in which the cryptanalyst possesses only ciphertext.

A *known plaintext attack* is a cryptanalytic attack in which the cryptanalyst possesses a substantial quantity of corresponding plaintext and ciphertext.

A *chosen plaintext attack* is a cryptanalytic attack in which the cryptanalyst can submit an unlimited number of plaintext messages of his own choosing and examine the resulting cryptograms.

In all cases it is assumed that the opponent knows the general system $\{S_K\}$ in use since this information can be obtained by studying a cryptographic device. While many users of cryptography attempt to keep their equipment secret, many commercial applications require not only that the general system be public but that it be standard.

A ciphertext only attack occurs frequently in practice. The cryptanalyst uses only knowledge of the statistical properties of the language in use (e.g., in English, the letter e occurs 13 percent of the time) and knowledge of certain "probable" words (e.g., a letter probably begins "Dear Sir:"). It is the weakest threat to which a system can be subjected, and any system which succumbs to it is considered totally insecure.

A system's use product encrypted messages section. This system's use product encrypted messages section. This system's use product encrypted messages section.

A chosen practice, ting a pr phering i which is s its users plant me.

For th approprie threats a working e the assess tems whic attack ca text or ch

As is c system id chosen. pl system id subjects i as autom to build s identify.

The ch tack, terr developm foe" syste military r planes au challenge encrypts i the radar encrypted a friendly ritory, en amine the the authe plaintext countered need not

There a cannot be which req introduce receiver's ion in mu

combi-
way that
change
ily with
perty is
used to
receiver.
ting to-
nel, but
uthentic
essages
system
prevent
ormation
age and
example,
and enat
only
message
late and
ystem in
in large
nal error
of noise
le 7" into
also cor-
age will
ographic
are to be
crypto-
authenti-
attack in
t.
attack in
quantity
attack in
l number
mine the
nows the
on can be
nile many
quipment
only that
dard.
practice.
tatistical
the letter
of certain
ns "Dear
m can be
it is con-

A system which is secure against a known plaintext attack frees its users from the need to keep their past messages secret, or to paraphrase them prior to declassification. This is an unreasonable burden to place on the system's users, particularly in commercial situations where product announcements or press releases may be sent in encrypted form for later public disclosure. Similar situations in diplomatic correspondence have led to the cracking of many supposedly secure systems. While a known plaintext attack is not always possible, its occurrence is frequent enough that a system which cannot resist it is not considered secure.

A chosen plaintext attack is difficult to achieve in practice, but can be approximated. For example, submitting a proposal to a competitor may result in his enciphering it for transmission to his headquarters. A cipher which is secure against a chosen plaintext attack thus frees its users from concern over whether their opponents can plant messages in their system.

For the purpose of certifying systems as secure, it is appropriate to consider the more formidable cryptanalytic threats as these not only give more realistic models of the working environment of a cryptographic system, but make the assessment of the system's strength easier. Many systems which are difficult to analyze using a ciphertext only attack can be ruled out immediately under known plaintext or chosen plaintext attacks.

As is clear from these definitions, cryptanalysis is a system identification problem. The known plaintext and chosen plaintext attacks correspond to passive and active system identification problems, respectively. Unlike many subjects in which system identification is considered, such as automatic fault diagnosis, the goal in cryptography is to build systems which are difficult, rather than easy, to identify.

The chosen plaintext attack is often called an IFF attack, terminology which descends from its origin in the development of cryptographic "identification friend or foe" systems after World War II. An IFF system enables military radars to distinguish between friendly and enemy planes automatically. The radar sends a time-varying challenge to the airplane which receives the challenge, encrypts it under the appropriate key, and sends it back to the radar. By comparing this response with a correctly encrypted version of the challenge, the radar can recognize a friendly aircraft. While the aircraft are over enemy territory, enemy cryptanalysts can send challenges and examine the encrypted responses in an attempt to determine the authentication key in use, thus mounting a chosen plaintext attack on the system. In practice, this threat is countered by restricting the form of the challenges, which need not be unpredictable, but only nonrepeating.

There are other threats to authentication systems which cannot be treated by conventional cryptography, and which require recourse to the new ideas and techniques introduced in this paper. The *threat of compromise of the receiver's authentication data* is motivated by the situation in multiuser networks where the receiver is often the

system itself. The receiver's password tables and other authentication data are then more vulnerable to theft than those of the transmitter (an individual user). As shown later, some techniques for protecting against this threat also protect against the *threat of dispute*. That is, a message may be sent but later repudiated by either the transmitter or the receiver. Or, it may be alleged by either party that a message was sent when in fact none was. Unforgeable digital signatures and receipts are needed. For example, a dishonest stockbroker might try to cover up unauthorized buying and selling for personal gain by forging orders from clients, or a client might disclaim an order actually authorized by him but which he later sees will cause a loss. We will introduce concepts which allow the receiver to verify the authenticity of a message, but prevent him from generating apparently authentic messages, thereby protecting against both the threat of compromise of the receiver's authentication data and the threat of dispute.

III. PUBLIC KEY CRYPTOGRAPHY

As shown in Fig. 1, cryptography has been a derivative security measure. Once a secure channel exists along which keys can be transmitted, the security can be extended to other channels of higher bandwidth or smaller delay by encrypting the messages sent on them. The effect has been to limit the use of cryptography to communications among people who have made prior preparation for cryptographic security.

In order to develop large, secure, telecommunications systems, this must be changed. A large number of users n results in an even larger number, $(n^2 - n)/2$ potential pairs who may wish to communicate privately from all others. It is unrealistic to assume either that a pair of users with no prior acquaintance will be able to wait for a key to be sent by some secure physical means, or that keys for all $(n^2 - n)/2$ pairs can be arranged in advance. In another paper [5], the authors have considered a conservative approach requiring no new development in cryptography itself, but this involves diminished security, inconvenience, and restriction of the network to a starlike configuration with respect to initial connection protocol.

We propose that it is possible to develop systems of the type shown in Fig. 2, in which two parties communicating solely over a public channel and using only publicly known techniques can create a secure connection. We examine two approaches to this problem, called public key cryptosys-

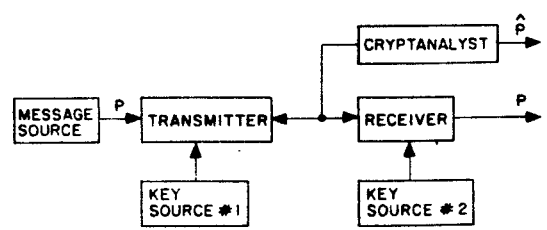


Fig. 2. Flow of information in public key system.

tems and public key distribution systems, respectively. The first are more powerful, lending themselves to the solution of the authentication problems treated in the next section, while the second are much closer to realization.

A *public key cryptosystem* is a pair of families $\{E_K\}_{K \in \{K\}}$ and $\{D_K\}_{K \in \{K\}}$ of algorithms representing invertible transformations,

$$E_K: \{M\} \rightarrow \{M\} \quad (2)$$

$$D_K: \{M\} \rightarrow \{M\} \quad (3)$$

on a finite message space $\{M\}$, such that

- 1) for every $K \in \{K\}$, E_K is the inverse of D_K ,
- 2) for every $K \in \{K\}$ and $M \in \{M\}$, the algorithms E_K and D_K are easy to compute,
- 3) for almost every $K \in \{K\}$, each easily computed algorithm equivalent to D_K is computationally infeasible to derive from E_K ,
- 4) for every $K \in \{K\}$, it is feasible to compute inverse pairs E_K and D_K from K .

Because of the third property, a user's enciphering key E_K can be made public without compromising the security of his secret deciphering key D_K . The cryptographic system is therefore split into two parts, a family of enciphering transformations and a family of deciphering transformations in such a way that, given a member of one family, it is infeasible to find the corresponding member of the other.

The fourth property guarantees that there is a feasible way of computing corresponding pairs of inverse transformations when no constraint is placed on what either the enciphering or deciphering transformation is to be. In practice, the cryptoequipment must contain a true random number generator (e.g., a noisy diode) for generating K , together with an algorithm for generating the $E_K - D_K$ pair from its outputs.

Given a system of this kind, the problem of key distribution is vastly simplified. Each user generates a pair of inverse transformations, E and D , at his terminal. The deciphering transformation D must be kept secret, but need never be communicated on any channel. The enciphering key E can be made public by placing it in a public directory along with the user's name and address. Anyone can then encrypt messages and send them to the user, but no one else can decipher messages intended for him. Public key cryptosystems can thus be regarded as *multiple access ciphers*.

It is crucial that the public file of enciphering keys be protected from unauthorized modification. This task is made easier by the public nature of the file. Read protection is unnecessary and, since the file is modified infrequently, elaborate write protection mechanisms can be economically employed.

A suggestive, although unfortunately useless, example of a public key cryptosystem is to encipher the plaintext, represented as a binary n -vector m , by multiplying it by an invertible binary $n \times n$ matrix E . The cryptogram thus

equals Em . Letting $D = E^{-1}$ we have $m = Dc$. Thus, both enciphering and deciphering require about n^2 operations. Calculation of D from E , however, involves a matrix inversion which is a harder problem. And it is at least conceptually simpler to obtain an arbitrary pair of inverse matrices than it is to invert a given matrix. Start with the identity matrix I and do elementary row and column operations to obtain an arbitrary invertible matrix E . Then starting with I do the inverses of these same elementary operations in reverse order to obtain $D = E^{-1}$. The sequence of elementary operations could be easily determined from a random bit string.

Unfortunately, matrix inversion takes only about n^3 operations. The ratio of "cryptanalytic" time (i.e., computing D from E) to enciphering or deciphering time is thus at most n , and enormous block sizes would be required to obtain ratios of 10^6 or greater. Also, it does not appear that knowledge of the elementary operations used to obtain E from I greatly reduces the time for computing D . And, since there is no round-off error in binary arithmetic, numerical stability is unimportant in the matrix inversion. In spite of its lack of practical utility, this matrix example is still useful for clarifying the relationships necessary in a public key cryptosystem.

A more practical approach to finding a pair of easily computed inverse algorithms E and D ; such that D is hard to infer from E , makes use of the difficulty of analyzing programs in low level languages. Anyone who has tried to determine what operation is accomplished by someone else's machine language program knows that E itself (i.e., what E does) can be hard to infer from an algorithm for E . If the program were to be made purposefully confusing through addition of unneeded variables and statements, then determining an inverse algorithm could be made very difficult. Of course, E must be complicated enough to prevent its identification from input-output pairs.

Essentially what is required is a one-way compiler: one which takes an easily understood program written in a high level language and translates it into an incomprehensible program in some machine language. The compiler is one-way because it must be feasible to do the compilation, but infeasible to reverse the process. Since efficiency in size of program and run time are not crucial in this application, such compilers may be possible if the structure of the machine language can be optimized to assist in the confusion.

Merkle [1] has independently studied the problem of distributing keys over an insecure channel. His approach is different from that of the public key cryptosystems suggested above, and will be termed a *public key distribution system*. The goal is for two users, A and B , to securely exchange a key over an insecure channel. This key is then used by both users in a normal cryptosystem for both enciphering and deciphering. Merkle has a solution whose cryptanalytic cost grows as n^2 where n is the cost to the legitimate users. Unfortunately the cost to the legitimate users of the system is as much as n transmission times as in computation, because Merkle's protocol requires n

potentially decided overhead practice. protocol of applications become a be achieved tical value

We now which has "key" to appears to users. An informat and vice only mer authentic Merkle's identities

The ne of comput prime nu

where a referred

A

Calculat: multiplic 18,

Computi: difficult

quires on algorithm The se difficulty rithm wh system v problem it might i For now

computin: that $q^{1/2}$

for a prop Each u X_i chosen 1}. Each l

in a publ and j wis

potential keys to be transmitted before one key can be decided on. Merkle notes that this high transmission overhead prevents the system from being very useful in practice. If a one megabit limit is placed on the setup protocol's overhead, his technique can achieve cost ratios of approximately 10 000 to 1, which are too small for most applications. If inexpensive, high bandwidth data links become available, ratios of a million to one or greater could be achieved and the system would be of substantial practical value.

We now suggest a new public key distribution system which has several advantages. First, it requires only one "key" to be exchanged. Second, the cryptanalytic effort appears to grow exponentially in the effort of the legitimate users. And, third, its use can be tied to a public file of user information which serves to authenticate user *A* to user *B* and vice versa. By making the public file essentially a read only memory, one personal appearance allows a user to authenticate his identity many times to many users. Merkle's technique requires *A* and *B* to verify each other's identities through other means.

The new technique makes use of the apparent difficulty of computing logarithms over a finite field $GF(q)$ with a prime number q of elements. Let

$$Y = \alpha^X \text{ mod } q, \quad \text{for } 1 \leq X \leq q - 1, \quad (4)$$

where α is a fixed primitive element of $GF(q)$, then X is referred to as the logarithm of Y to the base α , mod q :

$$X = \log_{\alpha} Y \text{ mod } q, \quad \text{for } 1 \leq Y \leq q - 1. \quad (5)$$

Calculation of Y from X is easy, taking at most $2 \times \log_2 q$ multiplications [6, pp. 398-422]. For example, for $X = 18$,

$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2. \quad (6)$$

Computing X from Y , on the other hand can be much more difficult and, for certain carefully chosen values of q , requires on the order of $q^{1/2}$ operations, using the best known algorithm [7, pp. 9, 575-576], [8].

The security of our technique depends crucially on the difficulty of computing logarithms mod q , and if an algorithm whose complexity grew as $\log_2 q$ were to be found, our system would be broken. While the simplicity of the problem statement might allow such simple algorithms, it might instead allow a proof of the problem's difficulty. For now we assume that the best known algorithm for computing logs mod q is in fact close to optimal and hence that $q^{1/2}$ is a good measure of the problem's complexity, for a properly chosen q .

Each user generates an independent random number X_i chosen uniformly from the set of integers $\{1, 2, \dots, q - 1\}$. Each keeps X_i secret, but places

$$Y_i = \alpha^{X_i} \text{ mod } q \quad (7)$$

in a public file with his name and address. When users i and j wish to communicate privately, they use

$$K_{ij} = \alpha^{X_i X_j} \text{ mod } q \quad (8)$$

as their key. User i obtains K_{ij} by obtaining Y_j from the public file and letting

$$K_{ij} = Y_j^{X_i} \text{ mod } q \quad (9)$$

$$= (\alpha^{X_j})^{X_i} \text{ mod } q \quad (10)$$

$$= \alpha^{X_j X_i} = \alpha^{X_i X_j} \text{ mod } q. \quad (11)$$

User j obtains K_{ij} in the similar fashion

$$K_{ij} = Y_i^{X_j} \text{ mod } q. \quad (12)$$

Another user must compute K_{ij} from Y_i and Y_j , for example, by computing

$$K_{ij} = Y_i^{(\log_{\alpha} Y_j)} \text{ mod } q. \quad (13)$$

We thus see that if logs mod q are easily computed the system can be broken. While we do not currently have a proof of the converse (i.e., that the system is secure if logs mod q are difficult to compute), neither do we see any way to compute K_{ij} from Y_i and Y_j without first obtaining either X_i or X_j .

If q is a prime slightly less than 2^b , then all quantities are representable as b bit numbers. Exponentiation then takes at most $2b$ multiplications mod q , while by hypothesis taking logs requires $q^{1/2} = 2^{b/2}$ operations. The cryptanalytic effort therefore grows exponentially relative to legitimate efforts. If $b = 200$, then at most 400 multiplications are required to compute Y_i from X_i , or K_{ij} from Y_i and X_j , yet taking logs mod q requires 2^{100} or approximately 10^{30} operations.

IV. ONE-WAY AUTHENTICATION

The problem of authentication is perhaps an even more serious barrier to the universal adoption of telecommunications for business transactions than the problem of key distribution. Authentication is at the heart of any system involving contracts and billing. Without it, business cannot function. Current electronic authentication systems cannot meet the need for a purely digital, unforgeable, message dependent signature. They provide protection against third party forgeries, but do not protect against disputes between transmitter and receiver.

In order to develop a system capable of replacing the current written contract with some purely electronic form of communication, we must discover a digital phenomenon with the same properties as a written signature. It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it. We will call any such technique *one-way authentication*. Since any digital signal can be copied precisely, a true digital signature must be recognizable without being known.

Consider the "login" problem in a multiuser computer system. When setting up his account, the user chooses a password which is entered into the system's password directory. Each time he logs in, the user is again asked to provide his password. By keeping this password secret from all other users, forged logins are prevented. This,

however, makes it vital to preserve the security of the password directory since the information it contains would allow perfect impersonation of any user. The problem is further compounded if system operators have legitimate reasons for accessing the directory. Allowing such legitimate accesses, but preventing all others, is next to impossible.

This leads to the apparently impossible requirement for a new login procedure capable of judging the authenticity of passwords without actually knowing them. While appearing to be a logical impossibility, this proposal is easily satisfied. When the user first enters his password PW , the computer automatically and transparently computes a function $f(PW)$ and stores this, not PW , in the password directory. At each successive login, the computer calculates $f(X)$, where X is the proffered password, and compares $f(X)$ with the stored value $f(PW)$. If and only if they are equal, the user is accepted as being authentic. Since the function f must be calculated once per login, its computation time must be small. A million instructions (costing approximately \$0.10 at bicentennial prices) seems to be a reasonable limit on this computation. If we could ensure, however, that calculation of f^{-1} required 10^{30} or more instructions, someone who had subverted the system to obtain the password directory could not in practice obtain PW from $f(PW)$, and could thus not perform an unauthorized login. Note that $f(PW)$ is not accepted as a password by the login program since it will automatically compute $f(f(PW))$ which will not match the entry $f(PW)$ in the password directory.

We assume that the function f is public information, so that it is not ignorance of f which makes calculation of f^{-1} difficult. Such functions are called one-way functions and were first employed for use in login procedures by R. M. Needham [9, p. 91]. They are also discussed in two recent papers [10], [11] which suggest interesting approaches to the design of one-way functions.

More precisely, a function f is a *one-way function* if, for any argument x in the domain of f , it is easy to compute the corresponding value $f(x)$, yet, for almost all y in the range of f , it is computationally infeasible to solve the equation $y = f(x)$ for any suitable argument x .

It is important to note that we are defining a function which is not invertible from a computational point of view, but whose noninvertibility is entirely different from that normally encountered in mathematics. A function f is normally called "noninvertible" when the inverse of a point y is not unique, (i.e., there exist distinct points x_1 and x_2 such that $f(x_1) = y = f(x_2)$). We emphasize that this is not the sort of inversion difficulty that is required. Rather, it must be overwhelmingly difficult, given a value y and knowledge of f , to calculate any x whatsoever with the property that $f(x) = y$. Indeed, if f is noninvertible in the usual sense, it may make the task of finding an inverse image easier. In the extreme, if $f(x) \equiv y_0$ for all x in the domain, then the range of f is $\{y_0\}$, and we can take any x as $f^{-1}(y_0)$. It is therefore necessary that f not be too degenerate. A small degree of degeneracy is tolerable and, as

discussed later, is probably present in the most promising class of one-way functions.

Polynomials offer an elementary example of one-way functions. It is much harder to find a root x_0 of the polynomial equation $p(x) = y$ than it is to evaluate the polynomial $p(x)$ at $x = x_0$. Purdy [11] has suggested the use of sparse polynomials of very high degree over finite fields, which appear to have very high ratios of solution to evaluation time. The theoretical basis for one-way functions is discussed at greater length in Section VI. And, as shown in Section V, one-way functions are easy to devise in practice.

The one-way function login protocol solves only some of the problems arising in a multiuser system. It protects against compromise of the system's authentication data when it is not in use, but still requires the user to send the true password to the system. Protection against eavesdropping must be provided by additional encryption, and protection against the threat of dispute is absent altogether.

A public key cryptosystem can be used to produce a true one-way authentication system as follows. If user A wishes to send a message M to user B , he "deciphers" it in his secret deciphering key and sends $D_A(M)$. When user B receives it, he can read it, and be assured of its authenticity by "enciphering" it with user A 's public enciphering key E_A . B also saves $D_A(M)$ as proof that the message came from A . Anyone can check this claim by operating on $D_A(M)$ with the publicly known operation E_A to recover M . Since only A could have generated a message with this property, the solution to the one-way authentication problem would follow immediately from the development of public key cryptosystems.

One-way message authentication has a partial solution suggested to the authors by Leslie Lamport of Massachusetts Computer Associates. This technique employs a one-way function f mapping k -dimensional binary space into itself for k on the order of 100. If the transmitter wishes to send an N bit message he generates $2N$, randomly chosen, k -dimensional binary vectors $x_1, X_1, x_2, X_2, \dots, x_N, X_N$ which he keeps secret. The receiver is given the corresponding images under f , namely $y_1, Y_1, y_2, Y_2, \dots, y_N, Y_N$. Later, when the message $m = (m_1, m_2, \dots, m_N)$ is to be sent, the transmitter sends x_1 or X_1 depending on whether $m_1 = 0$ or 1. He sends x_2 or X_2 depending on whether $m_2 = 0$ or 1, etc. The receiver operates with f on the first received block and sees whether it yields y_1 or Y_1 as its image and thus learns whether it was x_1 or X_1 , and whether $m_1 = 0$ or 1. In a similar manner the receiver is able to determine m_2, m_3, \dots, m_N . But the receiver is incapable of forging a change in even one bit of m .

This is only a partial solution because of the approximately 100-fold data expansion required. There is, however, a modification which eliminates the expansion problem when N is roughly a megabit or more. Let g be a one-way mapping from binary N -space to binary n -space where n is approximately 50. Take the N bit message m

and operate on use the previous $k = 100$, this message. It th during transn of y_1, Y_1, \dots ; a large number with the same of g makes th thus to forge. a normal one- m' but also o even given n Finding such Section V).

There is an authenticatio X which he ke f is a one-wa thenticator is tem by apply past respons The problem amount of c many orders example t is must work fo million. Both an average of mountable, t nique. The p for calculatin as $X^8 = ((X: t$ and t would may be, how f from being

V. PROBI

In this sec graphic prof others, ther difficulty. W of trap doors

In Sector intended for tication agai be used to c

A crypto: plaintext at tion.

As indicat $\{C\}_{K \in \{K\}}$ wh fix $P = P_0$ a:

nising
e-way
poly-
poly-
use of
fields,
eval-
ctions
shown
ise in
some
otects
n data
nd the
eaves-
m, and
t alto-
a true
wishes
in his
user B
enticity
ng key
e came
ing on
reover
ith this
ication
pment
olution
Massa-
ploys a
y space
mitter
N, ran-
vectors
The re-
namely
ge $m =$
ds x_1 or
 x_2 or X_2
iver op-
whether
er it was
nner the
t the re-
e bit of
approx-
is, how-
pansion
et g be a
n-space
essage m

and operate on it with g to obtain the n bit vector m' . Then use the previous scheme to send m' . If $N = 10^6$, $n = 50$, and $k = 100$, this adds $kn = 5000$ authentication bits to the message. It thus entails only a 5 percent data expansion during transmission (or 15 percent if the initial exchange of $y_1, Y_1, \dots, y_N, Y_N$ is included). Even though there are a large number of other messages (2^{N-n} on the average) with the same authentication sequence, the one-wayness of g makes them computationally infeasible to find and thus to forge. Actually g must be somewhat stronger than a normal one-way function, since an opponent has not only m' but also one of its inverse images m . It must be hard even given m to find a different inverse image of m' . Finding such functions appears to offer little trouble (see Section V).

There is another partial solution to the one-way user authentication problem. The user generates a password X which he keeps secret. He gives the system $f^T(X)$, where f is a one-way function. At time t the appropriate authenticator is $f^{T-t}(X)$, which can be checked by the system by applying $f^t(X)$. Because of the one-wayness of f , past responses are of no value in forging a new response. The problem with this solution is that it can require a fair amount of computation for legitimate login (although many orders of magnitude less than for forgery). If for example t is incremented every second and the system must work for one month on each password then $T = 2.6$ million. Both the user and the system must then iterate f an average of 1.3 million times per login. While not insurmountable, this problem obviously limits use of the technique. The problem could be overcome if a simple method for calculating $f^{(2^n)}$, for $n = 1, 2, \dots$ could be found, much as $X^8 = ((X^2)^2)^2$. For then binary decompositions of $T - t$ and t would allow rapid computation of f^{T-t} and f^t . It may be, however, that rapid computation of f^n precludes f from being one-way.

V. PROBLEM INTERRELATIONS AND TRAP DOORS

In this section, we will show that some of the cryptographic problems presented thus far can be reduced to others, thereby defining a loose ordering according to difficulty. We also introduce the more difficult problem of trap doors.

In Section II we showed that a cryptographic system intended for privacy can also be used to provide authentication against third party forgeries. Such a system can be used to create other cryptographic objects, as well.

A cryptosystem which is secure against a known plaintext attack can be used to produce a one-way function.

As indicated in Fig. 3, take the cryptosystem $\{S_K: \{P\} \rightarrow \{C\} \mid K \in \{K\}\}$ which is secure against a known plaintext attack, fix $P = P_0$ and consider the map

$$f: \{K\} \rightarrow \{C\} \tag{14}$$

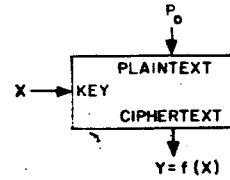


Fig. 3. Secure cryptosystem used as one-way function.

defined by

$$f(X) = S_X(P_0). \tag{15}$$

This function is one-way because solving for X given $f(X)$ is equivalent to the cryptanalytic problem of finding the key from a single known plaintext-ciphertext pair. Public knowledge of f is now equivalent to public knowledge of $\{S_K\}$ and P_0 .

While the converse of this result is not necessarily true, it is possible for a function originally found in the search for one-way functions to yield a good cryptosystem. This actually happened with the discrete exponential function discussed in Section III [8].

One-way functions are basic to both block ciphers and key generators. A key generator is a pseudorandom bit generator whose output, the keystream, is added modulo 2 to a message represented in binary form, in imitation of a one-time pad. The key is used as a "seed" which determines the pseudorandom keystream sequence. A known plaintext attack thus reduces to the problem of determining the key from the keystream. For the system to be secure, computation of the key from the keystream must be computationally infeasible. While, for the system to be usable, calculation of the keystream from the key must be computationally simple. Thus a good key generator is, almost by definition, a one-way function.

Use of either type of cryptosystem as a one way function suffers from a minor problem. As noted earlier, if the function f is not uniquely invertible, it is not necessary (or possible) to find the actual value of X used. Rather any X with the same image will suffice. And, while each mapping S_K in a cryptosystem must be bijective, there is no such restriction on the function f from key to ciphertext defined above. Indeed, guaranteeing that a cryptosystem has this property appears quite difficult. In a good cryptosystem the mapping f can be expected to have the characteristics of a randomly chosen mapping (i.e., $f(X_i)$ is chosen uniformly from all possible Y , and successive choices are independent). In this case, if X is chosen uniformly and there are an equal number of keys and messages (X and Y), then the probability that the resultant Y has $k + 1$ inverses is approximately $e^{-1/k!}$ for $k = 0, 1, 2, 3, \dots$. This is a Poisson distribution with mean $\lambda = 1$, shifted by 1 unit. The expected number of inverses is thus only 2. While it is possible for f to be more degenerate, a good cryptosystem will not be too degenerate since then the key is not being well used. In the worst case, if $f(X) \equiv Y_0$ for some Y_0 , we have $S_K(P_0) \equiv C_0$, and encipherment of P_0 would not depend on the key at all!

While we are usually interested in functions whose domain and range are of comparable size, there are exceptions. In the previous section we required a one-way function mapping long strings onto much shorter ones. By using a block cipher whose key length is larger than the blocksize, such functions can be obtained using the above technique.

Evans *et al.* [10] have a different approach to the problem of constructing a one-way function from a block cipher. Rather than selecting a fixed P_0 as the input, they use the function

$$f(X) = S_X(X). \quad (16)$$

This is an attractive approach because equations of this form are generally difficult to solve, even when the family S is comparatively simple. This added complexity, however, destroys the equivalence between the security of the system S under a known plaintext attack and the one-wayness of f .

Another relationship has already been shown in Section IV.

A public key cryptosystem can be used to generate a one-way authentication system.

The converse does not appear to hold, making the construction of a public key cryptosystem a strictly more difficult problem than one-way authentication. Similarly, a public key cryptosystem can be used as a public key distribution system, but not conversely.

Since in a public key cryptosystem the general system in which E and D are used must be public, specifying E specifies a complete algorithm for transforming input messages into output cryptograms. As such a public key system is really a set of *trap-door one-way functions*. These are functions which are not really one-way in that simply computed inverses exist. But given an algorithm for the forward function it is computationally infeasible to find a simply computed inverse. Only through knowledge of certain *trap-door information* (e.g., the random bit string which produced the E - D pair) can one easily find the easily computed inverse.

Trap doors have already been seen in the previous paragraph in the form of *trap-door one-way functions*, but other variations exist. A *trap-door cipher* is one which strongly resists cryptanalysis by anyone not in possession of *trap-door information* used in the design of the cipher. This allows the designer to break the system after he has sold it to a client and yet falsely to maintain his reputation as a builder of secure systems. It is important to note that it is not greater cleverness or knowledge of cryptography which allows the designer to do what others cannot. If he were to lose the trap-door information he would be no better off than anyone else. The situation is precisely analogous to a combination lock. Anyone who knows the combination can do in seconds what even a skilled locksmith would require hours to accomplish. And yet, if he forgets the combination, he has no advantage.

A trap-door cryptosystem can be used to produce a public key distribution system.

For A and B to establish a common private key, A chooses a key at random and sends an arbitrary plaintext-cryptogram pair to B . B , who made the trap-door cipher public, but kept the trap-door information secret, uses the plaintext-cryptogram pair to solve for the key. A and B now have a key in common.

There is currently little evidence for the existence of trap-door ciphers. However they are a distinct possibility and should be remembered when accepting a cryptosystem from a possible opponent [12].

By definition, we will require that a trap-door problem be one in which it is computationally feasible to devise the trap door. This leaves room for yet a third type of entity for which we shall use the prefix "quasi." For example a *quasi one-way function* is not one-way in that an easily computed inverse exists. However, it is computationally infeasible even for the designer, to find the easily computed inverse. Therefore a quasi one-way function can be used in place of a one-way function with essentially no loss in security.

Losing the trap-door information to a trap-door one-way function makes it into a quasi one-way function, but there may also be one-way functions not obtainable in this manner.

It is entirely a matter of definition that quasi one-way functions are excluded from the class of one-way functions. One could instead talk of one-way functions in the wide sense or in the strict sense.

Similarly, a quasi secure cipher is a cipher which will successfully resist cryptanalysis, even by its designer, and yet for which there exists a computationally efficient cryptanalytic algorithm (which is of course computationally infeasible to find). Again, from a practical point of view, there is essentially no difference between a secure cipher and a quasi secure one.

We have already seen that public key cryptosystems imply the existence of trap-door one-way functions. However the converse is not true. For a trap-door one-way function to be usable as a public key cryptosystem, it must be invertible (i.e., have a unique inverse.)

VI. COMPUTATIONAL COMPLEXITY

Cryptography differs from all other fields of endeavor in the ease with which its requirements may appear to be satisfied. Simple transformations will convert a legible text into an apparently meaningless jumble. The critic, who wishes to claim that meaning might yet be recovered by cryptanalysis, is then faced with an arduous demonstration if he is to prove his point of view correct. Experience has shown, however, that few systems can resist the concerted attack of skillful cryptanalysts, and many supposedly secure systems have subsequently been broken.

In consequence of this, judging the worth of new systems has always been a central concern of cryptographers. During the sixteenth and seventeenth centuries, mathematical arguments were often invoked to argue the strength of cryptographic methods, usually relying on counting methods which showed the astronomical number

of possible combinations to be laid to the gebräuchlichen (whose strength, then, the security of the certificate)

During the time of the connection [3] showed in use since the form of systems is a key which message (unwieldy key cryptosystem) be unconcealable always depends on the membership of the problem search.

The practical discipline: computation algorithm computation has concentrated studying progression in application one-way function

A function polynomial Turing Machine polynomial think of that it is more must be hard are problems pp. 405-4

There are which can technique unlimited may not be (for nondecreasing in polynomial one with a class NP) questions strictly larger

Among but not known traveling sales problem coloring problems

of possible keys. Though the problem is far too difficult to be laid to rest by such simple methods, even the noted algebraist Cardano fell into this trap [2, p. 145]. As systems whose strength had been so argued were repeatedly broken, the notion of giving mathematical proofs for the security of systems fell into disrepute and was replaced by certification via cryptanalytic assault.

During this century, however, the pendulum has begun to swing back in the other direction. In a paper intimately connected with the birth of information theory, Shannon [3] showed that the one time pad system, which had been in use since the late twenties offered "perfect secrecy" (a form of unconditional security). The provably secure systems investigated by Shannon rely on the use of either a key whose length grows linearly with the length of the message or on perfect source coding and are therefore too unwieldy for most purposes. We note that neither public key cryptosystems nor one-way authentication systems can be unconditionally secure because the public information always determines the secret information uniquely among the members of a finite set. With unlimited computation, the problem could therefore be solved by a straightforward search.

The past decade has seen the rise of two closely related disciplines devoted to the study of the costs of computation: computational complexity theory and the analysis of algorithms. The former has classified known problems in computing into broad classes by difficulty, while the latter has concentrated on finding better algorithms and studying the resources they consume. After a brief digression into complexity theory, we will examine its application to cryptography, particularly the analysis of one-way functions.

A function is said to belong to the complexity class P (for polynomial) if it can be computed by a deterministic Turing Machine in a time which is bounded above by some polynomial function of the length of its input. One might think of this as the class of easily computed functions, but it is more accurate to say that a function not in this class must be hard to compute for at least some inputs. There are problems which are known not to be in the class P [13, pp. 405-425].

There are many problems which arise in engineering which cannot be solved in polynomial time by any known techniques, unless they are run on a computer with an unlimited degree of parallelism. These problems may or may not belong to the class P , but belong to the class NP (for nondeterministic, polynomial) of problems solvable in polynomial time on a "nondeterministic" computer (i.e., one with an unlimited degree of parallelism). Clearly the class NP includes the class P , and one of the great open questions in complexity theory is whether the class NP is strictly larger.

Among the problems known to be solvable in NP time, but not known to be solvable in P time, are versions of the traveling salesman problem, the satisfiability problem for propositional calculus, the knapsack problem, the graph coloring problem, and many scheduling and minimization problems [13, pp. 363-404], [14]. We see that it is not lack

of interest or effort which has prevented people from finding solutions in P time for these problems. It is thus strongly believed that at least one of these problems must not be in the class P , and that therefore the class NP is strictly larger.

Karp has identified a subclass of the NP problems, called NP complete, with the property that if any one of them is in P , then all NP problems are in P . Karp lists 21 problems which are NP complete, including all of the problems mentioned above [14].

While the NP complete problems show promise for cryptographic use, current understanding of their difficulty includes only worst case analysis. For cryptographic purposes, typical computational costs must be considered. If, however, we replace worst case computation time with average or typical computation time as our complexity measure, the current proofs of the equivalences among the NP complete problems are no longer valid. This suggests several interesting topics for research. The ensemble and typicality concepts familiar to information theorists have an obvious role to play.

We can now identify the position of the general cryptanalytic problem among all computational problems.

The cryptanalytic difficulty of a system whose encryption and decryption operations can be done in P time cannot be greater than NP .

To see this, observe that any cryptanalytic problem can be solved by finding a key, inverse image, etc., chosen from a finite set. Choose the key nondeterministically and verify in P time that it is the correct one. If there are M possible keys to choose from, an M -fold parallelism must be employed. For example in a known plaintext attack, the plaintext is encrypted simultaneously under each of the keys and compared with the cryptogram. Since, by assumption, encryption takes only P time, the cryptanalysis takes only NP time.

We also observe that the general cryptanalytic problem is NP complete. This follows from the breadth of our definition of cryptographic problems. A one-way function with an NP complete inverse will be discussed next.

Cryptography can draw directly from the theory of NP complexity by examining the way in which NP complete problems can be adapted to cryptographic use. In particular, there is an NP complete problem known as the knapsack problem which lends itself readily to the construction of a one-way function.

Let $y = f(x) = a \cdot x$ where a is a known vector of n integers (a_1, a_2, \dots, a_n) and x is a binary n -vector. Calculation of y is simple, involving a sum of at most n integers. The problem of inverting f is known as the knapsack problem and requires finding a subset of the $\{a_i\}$ which sum to y .

Exhaustive search of all 2^n subsets grows exponentially and is computationally infeasible for n greater than 100 or so. Care must be exercised, however, in selecting the parameters of the problem to ensure that shortcuts are not possible. For example if $n = 100$ and each a_i is 32 bits long, y is at most 39 bits long, and f is highly degenerate; re-

quiring on the average only 2^{38} tries to find a solution. Somewhat more trivially, if $a_i = 2^{i-1}$ then inverting f is equivalent to finding the binary decomposition of y .

This example demonstrates both the great promise and the considerable shortcomings of contemporary complexity theory. The theory only tells us that the knapsack problem is probably difficult in the worst case. There is no indication of its difficulty for any particular array. It appears, however, that choosing the $\{a_i\}$ uniformly from $\{0, 1, 2, \dots, 2^n - 1\}$ results in a hard problem with probability one as $n \rightarrow \infty$.

Another potential one-way function, of interest in the analysis of algorithms, is exponentiation mod q , which was suggested to the authors by Prof. John Gill of Stanford University. The one-wayness of this functions has already been discussed in Section III.

VII. HISTORICAL PERSPECTIVE

While at first the public key systems and one-way authentication systems suggested in this paper appear to be unportended by past cryptographic developments, it is possible to view them as the natural outgrowth of trends in cryptography stretching back hundreds of years.

Secrecy is at the heart of cryptography. In early cryptography, however, there was a confusion about what was to be kept secret. Cryptosystems such as the Caesar cipher (in which each letter is replaced by the one three places further on, so A is carried to D , B to E , etc.) depended for their security on keeping the entire encryption process secret. After the invention of the telegraph [2, p. 191], the distinction between a general system and a specific key allowed the general system to be compromised, for example by theft of a cryptographic device, without compromising future messages enciphered in new keys. This principle was codified by Kerchoffs [2, p. 235] who wrote in 1881 that the compromise of a cryptographic system should cause no inconvenience to the correspondents. About 1960, cryptosystems were put into service which were deemed strong enough to resist a known plaintext cryptanalytic attack, thereby eliminating the burden of keeping old messages secret. Each of these developments decreased the portion of the system which had to be protected from public knowledge, eliminating such tedious expedients as paraphrasing diplomatic dispatches before they were presented. Public key systems are a natural continuation of this trend toward decreasing secrecy.

Prior to this century, cryptographic systems were limited to calculations which could be carried out by hand or with simple slide-rule-like devices. The period immediately after World War I saw the beginning of a revolutionary trend which is now coming to fruition. Special purpose machines were developed for enciphering. Until the development of general purpose digital hardware, however, cryptography was limited to operations which could be performed with simple electromechanical systems. The development of digital computers has freed it from the limitations of computing with gears and has allowed the search for better encryption methods according to purely cryptographic criteria.

The failure of numerous attempts to demonstrate the soundness of cryptographic systems by mathematical proof led to the paradigm of certification by cryptanalytic attack set down by Kerchoffs [2, p. 234] in the last century. Although some general rules have been developed, which aid the designer in avoiding obvious weaknesses, the ultimate test is an assault on the system by skilled cryptanalysts under the most favorable conditions (e.g., a chosen plaintext attack). The development of computers has led for the first time to a mathematical theory of algorithms which can begin to approach the difficult problem of estimating the computational difficulty of breaking a cryptographic system. The position of mathematical proof may thus come full circle and be reestablished as the best method of certification.

The last characteristic which we note in the history of cryptography is the division between amateur and professional cryptographers. Skill in production cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from the amateurs. Thomas Jefferson, a cryptographic amateur, invented a system which was still in use in World War II [2, pp. 192-195], while the most noted cryptographic system of the twentieth century, the rotor machine, was invented simultaneously by four separate people, all amateurs [2, pp. 415, 420, 422-424]. We hope this will inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly.

REFERENCES

- [1] R. Merkle, "Secure communication over an insecure channel," submitted to *Communications of the ACM*.
- [2] D. Kahn, *The Codebreakers, The Story of Secret Writing*. New York: Macmillan, 1967.
- [3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.
- [4] M. E. Hellman, "An extension of the Shannon theory approach to cryptography," submitted to *IEEE Trans. Inform. Theory*, Sept. 1975.
- [5] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," presented at National Computer Conference, New York, June 7-10, 1976.
- [6] D. Knuth, *The Art of Computer Programming, Vol. 2, Semi-Numerical Algorithms*. Reading, MA: Addison-Wesley, 1969.
- [7] —, *The Art of Computer Programming, Vol. 3, Sorting and Searching*. Reading, MA: Addison-Wesley, 1973.
- [8] S. Pohlig and M. E. Hellman, "An improved algorithm for computing algorithms in $GF(p)$ and its cryptographic significance," submitted to *IEEE Trans. Inform. Theory*.
- [9] M. V. Wilkes, *Time-Sharing Computer Systems*. New York: Elsevier, 1972.
- [10] A. Evans, Jr., W. Kantrowitz, and E. Weiss, "A user authentication system not requiring secrecy in the computer," *Communications of the ACM*, vol. 17, pp. 437-442, Aug. 1974.
- [11] G. B. Purdy, "A high security log-in procedure," *Communications of the ACM*, vol. 17, pp. 442-445, Aug. 1974.
- [12] W. Diffie and M. E. Hellman, "Cryptanalysis of the NBS data encryption standard" submitted to *Computer*, May 1976.
- [13] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*. Reading, MA: Addison-Wesley, 1974.
- [14] R. M. Karp, "Reducibility among combinatorial problems," in *Complexity of Computer Computations*. R. E. Miller and J. W. Thatcher, Eds. New York: Plenum, 1972, pp. 85-104.

Abstr
network
signal d
averag
functio
compre
distorti
is defin
exists a
networ
functio
their ev
coding
tion-de
channe

M
delays
matio
work t
in ord
source
value
compr
throug
reduce
signal
dom a
comm
tinuot
ductio
compr
levels
for ex
form,
store-
compu
system
In tj
 $\gamma(D)$ c

Manu
work wa
N00014
tional S
present
Notre I
The
gineerin
CA.

Exhibit V

The First Ten Years of Public-Key Cryptography

WHITFIELD DIFFIE

Invited Paper

Public-key cryptosystems separate the capacities for encryption and decryption so that 1) many people can encrypt messages in such a way that only one person can read them, or 2) one person can encrypt messages in such a way that many people can read them. This separation allows important improvements in the management of cryptographic keys and makes it possible to 'sign' a purely digital message.

Public key cryptography was discovered in the Spring of 1975 and has followed a surprising course. Although diverse systems were proposed early on, the ones that appear both practical and secure today are all very closely related and the search for new and different ones has met with little success. Despite this reliance on a limited mathematical foundation public-key cryptography is revolutionizing communication security by making possible secure communication networks with hundreds of thousands of subscribers.

Equally important is the impact of public key cryptography on the theoretical side of communication security. It has given cryptographers a systematic means of addressing a broad range of security objectives and pointed the way toward a more theoretical approach that allows the development of cryptographic protocols with proven security characteristics.

I. INITIAL DISCOVERIES

Public key cryptography was born in May 1975, the child of two problems and a misunderstanding.

- First came the problem of key distribution. If two people who have never met before are to communicate privately using conventional cryptographic means, they must somehow agree in advance on a key that will be known to themselves and to no one else.
- The second problem, apparently unrelated to the first, was the problem of signatures. Could a method be devised that would provide the recipient of a purely digital electronic message with a way of demonstrating to other people that it had come from a particular person, just as a written signature on a letter allows the recipient to hold the author to its contents?

On the face of it, both problems seem to demand the impossible. In the first case, if two people could somehow communicate a secret key from one to the other without ever having met, why could they not communicate their

Manuscript received January 19, 1988; revised March 25, 1988. The author is with Bell-Northern Research, Mountain View, CA 94039, USA.

IEEE Log Number 8821645.

message in secret? The second is no better. To be effective, a signature must be hard to copy. How then can a digital message, which can be copied perfectly, bear a signature?

The misunderstanding was mine and prevented me from rediscovering the conventional key distribution center. The virtue of cryptography, I reasoned, was that, unlike any other known security technology, it did not require trust in any party not directly involved in the communication, only trust in the cryptographic systems. What good would it do to develop impenetrable cryptosystems, I reasoned, if their users were forced to share their keys with a key distribution center that could be compromised by either burglary or subpoena.

The discovery consisted not of a solution, but of the recognition that the two problems, each of which seemed unsolvable by definition, could be solved at all and that the solutions to both problems came in one package.

First to succumb was the signature problem. The conventional use of cryptography to authenticate messages had been joined in the 1950s by two new applications, whose functions when combined constitute a signature.

Beginning in 1952, a group under the direction of Horst Feistel at the Air Force Cambridge Research Center began to apply cryptography to the military problem of distinguishing friendly from hostile aircraft. In traditional *Identification Friend or Foe* systems, a fire control radar determines the identity of an aircraft by challenging it, much as a sentry challenges a soldier on foot. If the airplane returns the correct identifying information, it is judged to be friendly, otherwise it is thought to be hostile or at best neutral. To allow the correct response to remain constant for any significant period of time, however, is to invite opponents to record a legitimate friendly response and play it back whenever they themselves are challenged. The approach taken by Feistel's group, and now used in the MK XII IFF system, is to vary the exchange cryptographically from encounter to encounter. The radar sends a randomly selected challenge and judges the aircraft by whether it receives a correctly encrypted response. Because the challenges are never repeated, previously recorded responses will not be judged correct by a challenging radar.

Later in the decade, this novel authentication technique was joined by another, which seems first to have been

applied by
This time th
Access con
sitivity of th
passwords
access to th
tem's users
table is fille
the images
one-way fu
For any pas
easily. Give
ever, it is e
produce it.
an intrude
words and
routine.

Challeng
tions prov
of threats.
efforts of
nication ch
event to e
challengin
an oppon
tographic
to fool any
the one-w
captures t
ing the rac
login mes
time.

I realiz
taneously
unable to
rectness.
way func
someone
wards and
would iss
and dema
the trapd
ment in t
an algori
readily ch
to seem n
by a mes
signature

It did r
function
key distri
form of t
the pers
form the
holder o
the oper
the forw
to comp
available
public-k

The co
tosystem
pairs [36

applied by Roger Needham of Cambridge University [112]. This time the problem was protecting computer passwords. Access control systems often suffer from the extreme sensitivity of their password tables. The tables gather all of the passwords together in one place and anyone who gets access to this information can impersonate any of the system's users. To guard against this possibility, the password table is filled not with the passwords themselves, but with the images of the passwords under a *one-way function*. A one-way function is easy to compute, but difficult to invert. For any password, the correct table entry can be calculated easily. Given an output from the one-way function, however, it is exceedingly difficult to find any input that will produce it. This reduces the value of the password table to an intruder tremendously, since its entries are not passwords and are not acceptable to the password verification routine.

Challenge and response identification and one-way functions provide protection against two quite different sorts of threats. Challenge and response identification resists the efforts of an eavesdropper who can spy on the communication channel. Since the challenge varies randomly from event to event, the spy is unable to replay it and fool the challenging radar. There is, however, no protection against an opponent who captures the radar and learns its cryptographic keys. This opponent can use what he has learned to fool any other radar that is keyed the same. In contrast, the one-way function defeats the efforts of an intruder who captures the system password table (analogous to capturing the radar) but succumbs to anyone who intercepts the login message because the password does not change with time.

I realized that the two goals might be achieved simultaneously if the challenger could pose questions that it was unable to answer, but whose answers it could judge for correctness. I saw the solution as a generalization of the one-way function: a *trap-door one-way function* that allowed someone in possession of secret information to go backwards and compute the function's inverse. The challenger would issue a value in the range of the one-way function and demand to know its inverse. Only the person who knew the trapdoor would be able to find the corresponding element in the domain, but the challenger, in possession of an algorithm for computing the one-way function, could readily check the answer. In the applications that later came to seem most important, the role of the challenge was played by a message and the process took on the character of a signature, a *digital signature*.

It did not take long to realize that the trap-door one-way function could also be applied to the baffling problem of key distribution. For someone in possession of the forward form of the one-way function to send a secret message to the person who knew the trapdoor, he had only to transform the message with the one-way function. Only the holder of the trap-door information would be able to invert the operation and recover the message. Because knowing the forward form of the function did not make it possible to compute the inverse, the function could be made freely available. It is this possibility that gave the field its name: *public-key cryptography*.

The concept that emerges is that of a *public-key cryptosystem*: a cryptosystem in which keys come in inverse pairs [36] and each pair of keys has two properties.

- Anything encrypted with one key can be decrypted with the other.
- Given one member of the pair, the *public key*, it is infeasible to discover the other, the *secret key*.

This separation of encryption and decryption makes it possible for the subscribers to a communication system to list their public keys in a "telephone directory" along with their names and addresses. This done, the solutions to the original problems can be achieved by simple protocols.

- One subscriber can send a private message to another simply by looking up the addressee's public key and using it to encrypt the message. Only the holder of the corresponding secret key can read such a message; even the sender, should he lose the plaintext, is incapable of extracting it from the ciphertext.
- A subscriber can sign a message by encrypting it with his own secret key. Anyone with access to the public key can verify that it must have been encrypted with the corresponding secret key, but this is of no help to him in creating (forging) a message with this property.

The first aspect of public-key cryptography greatly simplifies the management of keys, especially in large communication networks. In order for a pair of subscribers to communicate privately using conventional end-to-end cryptography, they must both have copies of the same cryptographic key and this key must be kept secret from anyone they do not wish to take into their confidence. If a network has only a few subscribers, each person simply stores one key for every other subscriber against the day he will need it, but for a large network, this is impractical.

In a network with n subscribers there are $n(n-1)/2$ pairs, each of which may require a key. This amounts to five thousand keys in a network with only a hundred subscribers, half a million in a network with one thousand, and twenty million billion in a network the size of the North American telephone system. It is unthinkable to distribute this many keys in advance and undesirable to postpone secure communication while they are carried from one party to the other by courier.

The second aspect makes it possible to conduct a much broader range of normal business practices over a telecommunication network. The availability of a signature that the receiver of a message cannot forge and the sender cannot readily disavow makes it possible to trust the network with negotiations and transactions of much higher value than would otherwise be possible.

It must be noted that both problems can be solved without public-key cryptography, but that conventional solutions come at a great price. Centralized *key distribution centers* can on request provide a subscriber with a key for communicating with any other subscriber and protocols for this purpose will be discussed later on. The function of the signature can also be approximated by a central registry that records all transactions and bears witness in cases of dispute. Both mechanisms, however, encumber the network with the intrusion of a third party into many conversations, diminishing security and degrading performance.

At the time public-key cryptography was discovered, I was working with Martin Hellman in the Electrical Engineering Department at Stanford University. It was our immediate reaction, and by no means ours alone, that the

problem of producing public-key cryptosystems would be quite difficult. Instead of attacking this problem in earnest, Marty and I forged ahead in examining the consequences.

The first result of this examination to reach a broad audience was a paper entitled "Multi-User Cryptographic Techniques" [35], which we gave at the National Computer Conference in 1976. We wrote the paper in December 1975 and sent preprints around immediately. One of the preprints went to Peter Blatman, a Berkeley graduate student and friend since childhood of cryptography's historian David Kahn. The result was to bring from the woodwork Ralph Merkle, possibly the single most inventive character in the public-key saga.

Merkle's Puzzles

Ralph Merkle had registered in the Fall of 1974 for Lance Hoffman's course in computer security at U.C. Berkeley. Hoffman wanted term papers and required each student to submit a proposal early in the term. Merkle addressed the problem of public-key distribution or as he called it "Secure Communication over Insecure Channels" [70]. Hoffman could not understand Merkle's proposal. He demanded that it be rewritten, but alas found the revised version no more comprehensible than the original. After one more iteration of this process, Merkle dropped the course, but he did not cease working on the problem despite continuing failure to make his results understood.

Although Merkle's original proposal may have been hard to follow, the idea is quite simple. Merkle's approach is to communicate a cryptographic key from one person to another by hiding it in a large collection of puzzles. Following the tradition in public-key cryptography the parties to this communication will be called Alice and Bob rather than the faceless A and B , X and Y , or I and J , common in technical literature.

Alice manufactures a million or more puzzles and sends them over the exposed communication channel to Bob. Each puzzle contains a cryptographic key in a recognizable standard format. The puzzle itself is a cryptogram produced by a block cipher with a fairly small key space. As with the number of puzzles, a million is a plausible number. When Bob receives the puzzles, he picks one and solves it, by the simple expedient of trying each of the block cipher's million keys in turn until he finds one that results in plaintext of the correct form. This requires a large but hardly impossible amount of work.

In order to inform Alice which puzzle he has solved, Bob uses the key it contains to encrypt a fixed test message, which he transmits to Alice. Alice now tries her million keys on the test message until she finds the one that works. This is the key from the puzzle Bob has chosen.

The task facing an intruder is more arduous. Rather than selecting one of the puzzles to solve, he must solve on average half of them. The amount of effort he must expend is therefore approximately the square of that expended by the legitimate communicators.

The n to n^2 advantage the legitimate communicators have over the intruder is small by cryptographic standards, but sufficient to make the system plausible in some circumstances. Suppose, for example, that the plaintext of each puzzle is 96 bits, consisting of 64 bits of key together with a thirty-two bit block of zeros that enables Bob to recognize the right solution. The puzzle is constructed by encrypting this plaintext using a block cipher with 20 bits of key. Alice

produces a million of the puzzles and Bob requires about half a million tests to solve one. The bandwidth and computing power required to make this feasible are large but not inaccessible. On a DS1 (1.544 Mbit) channel it would require about a minute to communicate the puzzles. If keys can be tried on the selected puzzle at about ten-thousand per second, it will take Bob another minute to solve it. Finally, it will take a similar amount of time for Alice to figure out, from the test message, which key has been chosen.

The intruder can expect to have to solve half a million puzzles at half a million tries apiece. With equivalent computational facilities, this requires twenty-five million seconds or about a year. For applications such as authentication, in which the keys are no longer of use after communication is complete, the security of this system might be sufficient.

When Merkle saw the preprint of "Multi-User Cryptographic Techniques" he immediately realized he had found people who would appreciate his work and sent us copies of the paper he had been endeavoring unsuccessfully to publish. We in turn realized that Merkle's formulation of the problem was quite different from mine and, because Merkle had isolated one of the two intertwined problems I had seen, potentially simpler.

Even before the notion of putting trap-doors into one-way functions had appeared, a central objective of my work with Marty had been to identify and study functions that were easy to compute in one direction, but difficult to invert. Three principal examples of this simplest and most basic of cryptographic phenomena occupied our thoughts.

- John Gill, a colleague in the Electrical Engineering Department at Stanford, had suggested discrete exponentiation because the inverse problem, discrete logarithm, was considered very difficult.
- I had sought suitable problems in the chapter on NP-complete functions in Aho, Hopcroft, and Ullman's book on computational complexity [3] and selected the knapsack problem as most appropriate.
- Donald Knuth of the Stanford Computer Science Department had suggested that multiplying a pair of primes was easy, but that factoring the result, even when it was known to have precisely two factors, was exceedingly hard.

All three of these one-way functions were shortly to assume great importance.

II. EXPONENTIAL KEY EXCHANGE

The exponential example was tantalizing because of its combinatorial peculiarities. When I had first thought of digital signatures, I had attempted to achieve them with a scheme using tables of exponentials. This system failed, but Marty and I continued twisting exponentials around in our minds and discussions trying to make them fit. Marty eventually made the breakthrough early one morning in May 1976. I was working at the Stanford Artificial Intelligence Laboratory on the paper that we were shortly to publish under the title "New Directions in Cryptography" [36] when Marty called and explained exponential key exchange in its unnerving simplicity. Listening to him, I realized that the notion had been at the edge of my mind for some time, but had never really broken through.

Exponential key exchange takes advantage of the ease with which exponentials can be computed in a Galois (finite)

field $GF(q)$ with the diffi

Y

where α is a primitive element of $GF(q)$, the base α , over

$X = 1$

Calculation it takes at r

Computing difficult [1] extracting proportion

though after fairly quick needed to and will a

To initialize X_A un keeps X_A

to Bob. S sends the now com

and use t Y_B she of

and Bob

No one else is a major date no Y_A or Y_B

If q is multiplied Y_A over $GF(2^{100})$ (or

The restricted with 2^n

field $GF(q)$ with a prime number q or elements (the numbers $\{0, 1, \dots, q-1\}$ under arithmetic modulo q) as compared with the difficulty of computing logarithms in the same field. If

$$Y = \alpha^X \text{ mod } q, \quad \text{for } 1 < X < q - 1$$

where α is a fixed primitive element of $GF(q)$ (that is the powers of α produce all the nonzero elements $1, 2, \dots, q-1$ of $GF(q)$), then X is referred to as the logarithm of Y to the base α , over $GF(q)$:

$$X = \log_{\alpha} Y \text{ over } GF(q), \quad \text{for } 1 < Y < q - 1.$$

Calculation of Y from X is easy: Using repeated squaring, it takes at most $2 \times \log_2 q$ multiplications. For example

$$\begin{aligned} \alpha^{37} &= \alpha^{32+4+1} \\ &= \left(\left(\left(\alpha^2 \right)^2 \right)^2 \right)^2 \times (\alpha^2)^2 \times \alpha. \end{aligned}$$

Computing X from Y , on the other hand, is typically far more difficult [104], [83], [29]. If q has been chosen correctly, extracting logarithms modulo q requires a precomputation proportional to

$$L(q) = e^{\sqrt{\ln q \times \ln \ln q}},$$

though after that individual logarithms can be calculated fairly quickly. The function $L(q)$ also estimates the time needed to factor a composite number of comparable size and will appear again in that context.

To initiate communication Alice chooses a random number X_A uniformly from the integers $1, 2, \dots, q-1$. She keeps X_A secret, but sends

$$Y_A = \alpha^{X_A} \text{ mod } q$$

to Bob. Similarly, Bob chooses a random number X_B and sends the corresponding Y_B to Alice. Both Alice and Bob can now compute

$$K_{AB} = \alpha^{X_A X_B} \text{ mod } q$$

and use this as their key. Alice computes K_{AB} by raising the Y_B she obtained from Bob to the power X_A

$$\begin{aligned} K_{AB} &= Y_B^{X_A} \text{ mod } q \\ &= (\alpha^{X_B})^{X_A} \text{ mod } q \\ &= \alpha^{X_B X_A} = \alpha^{X_A X_B} \text{ mod } q \end{aligned}$$

and Bob obtains K_{AB} in a similar fashion

$$K_{AB} = Y_A^{X_B} \text{ mod } q.$$

No one except Alice and Bob knows either X_A or X_B so anyone else must compute K_{AB} from Y_A and Y_B alone. The equivalence of this problem to the discrete logarithm problem is a major open question in public-key cryptography. To date no easier solution than taking the logarithm of either Y_A or Y_B has been discovered.

If q is a prime about 1000 bits in length, only about 2000 multiplications of 1000-bit numbers are required to compute Y_A from X_A , or K_{AB} from Y_A and X_B . Taking logarithms over $GF(q)$, on the other hand, currently demands more than 2^{100} (or approximately 10^{30}) operations.

The arithmetic of exponential key exchange is not restricted to prime fields; it can also be done in Galois Fields with 2^n elements, or in prime product rings [103], [68]. The

"2" approach has been taken by several people [64], [117], [56] because arithmetic in these fields can be performed with linear shift registers and is much faster than arithmetic over large primes. It has turned out, however, that discrete logarithms can also be calculated much more quickly in "2" fields and so the sizes of the registers must be about 50 percent greater.

Marty and I immediately recognized that we had a far more compact solution to the key distribution problem than Merkle's puzzles and hastened to add it to both the upcoming National Computer Conference presentation and to "New Directions." The latter now contained a solution to each aspect of the public-key problem, though not the combined solution I had envisioned. It was sent off to the IEEE TRANSACTIONS ON INFORMATION THEORY prior to my departure for NCC and like all of our other papers was immediately circulated in preprint.

III. TRAP-DOOR KNAPSACKS

Later in the same year, Ralph Merkle began work on his best known contribution to public-key cryptography: building trapdoors into the knapsack one-way function to produce the trap-door knapsack public-key cryptosystem.

The knapsack problem is fancifully derived from the notion of packing gear into a knapsack. A shipping clerk faced with an odd assortment of packages and a freight container will naturally try to find a subset of the packages that fills the container exactly with no wasted space. The simplest case of this problem, and the one that has found application in cryptography is the one dimensional case: packing varying lengths of fishing rod into a tall thin tube.

Given a cargo vector of integers $\mathbf{a} = (a_1, a_2, \dots, a_n)$ it is easy to add up the elements of any specified subvector. Presented with an integer S , however, it is not easy to find a subvector of \mathbf{a} whose elements sum to S , even if such a subvector is known to exist. This *knapsack problem* is well known in combinatorics and is believed to be extremely difficult in general. It belongs to the class of NP-complete problems, problems thought not to be solvable in polynomial time on any deterministic computer.

I had previously identified the knapsack problem as a theoretically attractive basis for a one-way function. The cargo vector \mathbf{a} can be used to encipher an n -bit message $\mathbf{x} = (x_1, x_2, \dots, x_n)$ by taking the dot product $S = \mathbf{a} \cdot \mathbf{x}$ as the ciphertext. Because one element of the dot product is binary, this process is easy and simply requires n additions. Inverting the function by finding a binary vector \mathbf{x} such that $\mathbf{a} \cdot \mathbf{x} = S$ solves the knapsack problem and is thus believed to be computationally infeasible if \mathbf{a} is randomly chosen. Despite this difficulty in general, many cases of the knapsack problem are quite easy and Merkle contrived to build a trapdoor into the knapsack one-way function by starting with a simple cargo vector and converting it into a more complex form [71].

If the cargo vector \mathbf{a} is chosen so that each element is larger than the sum of the preceding elements, it is called *superincreasing* and its knapsack problem is particularly simple. (In the special case where the components are 1, 2, 4, 8, etc., this is the elementary operation of binary decomposition.) For example, if $\mathbf{a}' = (171, 197, 459, 1191, 2410)$ and $S' = 3798$ then x_5 must equal 1. If it were 0 then even if $x_1, x_2, x_3,$ and x_4 were all equal to 1, the dot product $\mathbf{a} \cdot \mathbf{x}$ would be too small. Since $x_5 = 1, S' - a'_5 = 3797 - 2410$

= 1387 must be a sum of a subset of the first four elements of a' . The fact that $1387 > a'_4 = 191$ means that x_4 too must equal 1. Finally $S' - a'_5 - a'_4 = 196 = a'_2$ so $x_3 = 0$, $x_2 = 1$, and $x_1 = 0$.

The simple cargo vector a' cannot be used as a public enciphering key because anyone can easily recover a vector x for which $x \cdot a' = S'$ from a' and S' by the process described above. The algorithm for generating keys therefore chooses a random superincreasing cargo vector a (with a hundred or more components) and keeps this vector secret. It also generates a random integer m , larger than $\sum a_i$, and a random integer w , relatively prime to m , whose inverse $w^{-1} \pmod m$ will be used in decryption. The public cargo vector or enciphering key a is produced by multiplying each component of a' by $w \pmod m$

$$a = wa' \pmod m.$$

Alice publishes a transposed version of a as her public key, but keeps the transposition, the simple cargo vector a' , the multiplier w and its inverse, and the modulus m secret as her private key.

When Bob wants to send the message x to Alice he computes and sends

$$S = a \cdot x.$$

Because

$$\begin{aligned} S' &= w^{-1}S \pmod m \\ &= w^{-1} \sum a_i x_i \pmod m \\ &= w^{-1} \sum (wa_i \pmod m) x_i \pmod m \\ &= \sum (w^{-1}wa_i \pmod m) x_i \pmod m \\ &= \sum a'_i x_i \pmod m \\ &= a' \cdot x \end{aligned}$$

when $m > \sum a_i$, Alice can use her secret information, w^{-1} and m , to transform any message S that has been enciphered with her public key into $S' = w^{-1} \times S$ and solve the easy knapsack problem $S' = a' \cdot x$ to obtain x .

For example, for the secret vector a' , above, the values $w = 2550$ and $m = 8443$, result in the public vector $a = (5457, 4213, 5316, 6013, 7439)$, which hides the structure present in a' .

This process can be iterated to produce a sequence of cargo vectors with more and more difficult knapsack problems by using transformations (w_1, m_1) , (w_2, m_2) , etc. The overall transformation that results is not, in general, equivalent to any single (w, m) transformation.

The trap-door knapsack system does not lend itself readily to the production of signatures because most elements S of the ciphertext space $\{0 \leq S \leq \sum a_i\}$, do not have inverse images. This does not interfere with the use of the system for sending private messages, but requires special adaptation for signature applications [71], [98]. Merkle had great confidence in even the single iteration knapsack system and posted a note on his office offering a \$100 reward to anyone who could break it.

IV. THE RSA SYSTEM

Unknown to us at the time we wrote "New Directions" were the three people who were to make the single most spectacular contribution to public-key cryptography: Ron-

ald Rivest, Adi Shamir, and Leonard Adleman. Ron Rivest had been a graduate student in computer science at Stanford while I was working on proving the correctness of programs at the Stanford Artificial Intelligence Laboratory. One of my colleagues in that work was Zohar Manna, who shortly returned to Israel and supervised the doctoral research of Adi Shamir, at the Weitzman Institute. Len Adleman was a native San Franciscan with both undergraduate and graduate degrees from U.C. Berkeley. Despite this web of near connections, not one of the three had previously crossed our paths and their names were unfamiliar.

When the New Directions paper reached MIT in the fall of 1976, the three took up the challenge of producing a full-fledged public-key cryptosystem. The process lasted several months during which Rivest proposed approaches, Adleman attacked them, and Shamir recalls doing some of each.

In May 1977 they were rewarded with success. After investigating a number of possibilities, some of which were later put forward by other researchers [67], [1], they had discovered how a simple piece of classical number theory could be made to solve the problem. The resulting paper [91] also introduced Alice and Bob, the first couple of cryptography [53].

The RSA cryptosystem is a block cipher in which the plaintexts and ciphertexts are integers between 0 and $N - 1$ for some N . It resembles the exponential key exchange system described above in using exponentiation in modular arithmetic for its enciphering and deciphering operations but, unlike that system, RSA must do its arithmetic not over prime numbers, but over composite ones.

Knowledge of a plaintext M , a modulus N , and an exponent e are sufficient to allow calculation of $M^e \pmod N$. Exponentiation, however, is a one-way function with respect to the extraction of roots as well as logarithms. Depending on the characteristics of N , M , and e , it may be very difficult to invert.

The RSA system makes use of the fact that finding large (e.g., 200 digit) prime numbers is computationally easy, but that factoring the product of two such numbers appears computationally infeasible. Alice creates her secret and public keys by selecting two very large prime numbers, P and Q , at random, and multiplying them together to obtain a *bicomposite* modulus N . She makes this product public together with a suitably chosen enciphering exponent e , but keeps the factors, P and Q secret.

The enciphering process of exponentiation modulo N can be carried out by anyone who knows N , but only Alice, who knows the factors of N , can reverse the process and decipher.

Using P and Q , Alice can compute the Euler totient function $\phi(N)$, which counts the number of integers between 1 and N that are relatively prime to N and consequently invertible in arithmetic modulo N . For a bicomposite number this is

$$\phi(N) = (P - 1)(Q - 1).$$

The quantity $\phi(N)$ plays a critical role in Euler's theorem, which says that for any number x that is invertible modulo N (and for large N that is almost all of them)

$$x^{\phi(N)} \equiv 1 \pmod N$$

or slightly more generally

$$x^{k\phi(N)+1} \equiv x \pmod{N}.$$

Using $\phi(N)$ Alice can calculate [60] a number d such that

$$e \times d \equiv 1 \pmod{\phi(N)}$$

which is equivalent to saying that

$$e \times d = k \times \phi(N) + 1.$$

When the cryptogram $M^e \pmod{N}$ is raised to the power d the result is

$$(M^e)^d = M^{ed} = M^{k\phi(N)+1} \equiv M \pmod{N}$$

the original plaintext M .

As a very small example, suppose $P = 17$ and $Q = 31$ are chosen so that $N = PQ = 527$ and $\phi(N) = (P-1)(Q-1) = 480$. If $e = 7$ is chosen then $d = 343$. ($7 \times 343 = 2401 = 5 \times 480 + 1$). And if $M = 2$ then

$$C = M^e \pmod{N} = 2^7 \pmod{527} = 128.$$

Note again that only the public information (e, N) is required for enciphering M . To decipher, the private key d is needed to compute

$$\begin{aligned} M &= C^d \pmod{N} \\ &= 128^{343} \pmod{527} \\ &= 128^{256} \times 128^{64} \times 128^{16} \times 128^4 \times 128^2 \times 128^1 \pmod{527} \\ &= 35 \times 256 \times 35 \times 101 \times 47 \times 128 \pmod{527} \\ &= 2 \pmod{527}. \end{aligned}$$

Just as the strength of the exponential key exchange system is not known to be equivalent to the difficulty of extracting discrete logarithms, the strength of RSA has not been proven equivalent to factoring. There might be some method of taking the e th root of M^e without calculating d and thus without providing information sufficient to factor. While at MIT in 1978, M. O. Rabin [86] produced a variant of RSA, subsequently improved by Hugh Williams of the University of Manitoba [113], that is equivalent to factoring. Rivest and I have independently observed [38], [92], however, that the precise equivalence Rabin has shown is a two-edged sword.

V. THE McELIECE CODING SCHEME

Within a short time yet another public-key system was to appear, this due to Robert J. McEliece of the Jet Propulsion Laboratory at Cal Tech [69]. McEliece's system makes use of the existence of a class of error correcting codes, the Goppa codes, for which a fast decoding algorithm is known. His idea was to construct a Goppa code and disguise it as a general linear code, whose decoding problem is NP-complete. There is a strong parallel here with the trapdoor knapsack system in which a superincreasing cargo vector, whose knapsack problem is simple to solve, is disguised as a general cargo vector whose knapsack problem is NP-complete.

In a knapsack system, the secret key consists of a superincreasing cargo vector v , together with the multiplier w and the modulus m that disguise it; in McEliece's system, the secret key consists of the generator matrix G for a Goppa code together with a nonsingular matrix S and a permutation matrix P that disguise it. The public key appears as the encoding matrix $G' = SGP$ of a general linear code.

- To encode a data block u into a message x , Alice multiplies it by Bob's public encoding matrix G' and adds a locally generated noise block z .
- To decode, Bob multiplies the received message x by P^{-1} , decodes xP^{-1} to get a word in the Goppa code and multiplies this by S^{-1} to recover Alice's data block.

McEliece's system has never achieved wide acceptance and has probably never even been considered for implementation in any real application. This may be because the public keys are quite large, requiring on the order of a million bits; it may be because the system entails substantial expansion of the data; or it may be because McEliece's system bears a frightening structural similarity to the knapsack systems whose fate we shall discover shortly.

VI. THE FALL OF THE KNAPSACKS

Nineteen eighty-two was the most exciting time for public-key cryptography since its spectacular first three years. In March, Adi Shamir sent out a research announcement: He had broken the single iteration Merkle-Hellman knapsack system [101], [102]. By applying new results of Lenstra at the Mathematische Centrum in Amsterdam, Shamir had learned how to take a public cargo vector and discover a w and m that would convert it back into a superincreasing "secret" cargo vector—not necessarily the same one the originator had used, but one that would suffice for decrypting messages encrypted with the public cargo vector.

Shamir's original attack was narrow. It seemed that perhaps its only consequence would be to strengthen the knapsack system by adding conditions to the construction rules for avoiding the new attack. The first response of Gustavus J. Simmons, whose work will dominate a later section, was that he could avoid Shamir's attack without even changing the cargo vector merely by a more careful choice of w and m [16]. He quickly learned, however, that Shamir's approach could be extended to break a far larger class of knapsack systems [16].

Crypto '82 revealed that several other people had continued down the trail Shamir had blazed. Shamir himself had reached the same conclusions. Andy Odlyzko and Jeff Lagarias at Bell Labs were on the same track and Len Adleman had not only devised an attack but programmed it on an Apple II. The substance of the attacks will not be treated here since it is central to another paper in this special section (E. F. Brickell and A. M. Odlyzko "Cryptanalysis: A Survey of Recent Results"). The events they engendered, however, will.

I had the pleasure of chairing the cryptanalysis session at Crypto '82 in which the various results were presented. Ironically, at the time I accepted the invitation to organize such a session, Shamir's announcement stood alone and knapsack systems were only one of the topics to be discussed. My original program ran into very bad luck, however. Of the papers initially scheduled only Donald Davies's talk on: "The Bombe at Bletchley Park," was actually presented. Nonetheless, the lost papers were more than replaced by presentations on various approaches to the knapsack problem.

Last on the program were Len Adleman and his computer, which had accepted a challenge on the first night of the conference. The hour passed; various techniques for attacking knapsack systems with different characteristics

were heard; and the Apple II sat on (able waiting to reveal the results of its labors. At last Adleman rose to speak mumbling something self-deprecatingly about "the theory first, the public humiliation later" and beginning to explain his work. All the while the figure of Carl Nicolai moved silently in the background setting up the computer and copying a sequence of numbers from its screen onto a transparency. At last another transparency was drawn from a sealed envelope and the results placed side by side on the projector. They were identical. The public humiliation was not Adleman's, it was knapsack's.

Ralph Merkle was not present, but Marty Hellman, who was, gamely arose to make a concession speech on their behalf. Merkle, always one to put his money where his mouth was, had long since paid Shamir the \$100 in prize money that he had placed on the table nearly six years before.

The press wrote that knapsacks were dead. I was skeptical but ventured that the results were sufficiently threatening that I felt "nobody should entrust anything of great value to a knapsack system unless he had a much deeper theory of their functioning than was currently available." Nor was Merkle's enthusiasm dampened. He promptly raised his bet and offered \$1000 to anyone who could break a multiple iteration knapsack [72].

It took two years, but in the end, Merkle had to pay [42]. The money was finally claimed by Ernie Brickell in the summer of 1984 when he announced the destruction of a knapsack system of forty iterations and a hundred weights in the cargo vector in about an hour of Cray-1 time [17]. That Fall I was forced to admit: "knapsacks are flat on their back."

Closely related techniques have also been applied to make a dramatic reduction in the time needed to extract discrete logarithms in fields of type $GF(2^n)$. This approach was pioneered by Blake, Fuji-Hara, Vanstone, and Mullin in Canada [10] and refined by Coppersmith in the U.S. [28]. A comprehensive survey of this field was given by Andy Odlyzko at Eurocrypt '84 [79].

VII. EARLY RESPONSES TO PUBLIC KEY

A copy of the MIT report [90] on the RSA cryptosystem was sent to Martin Gardner, *Mathematical Games* editor of *Scientific American*, shortly after it was printed. Gardner promptly published a column [48] based on his reading of both the MIT report and "New Directions." Bearing the title: "A New Kind of Cryptosystem That Would Take Millions of Years to Break," it began a confusion that persists to this day between the two directions explored by the "New Directions" paper: public-key cryptography and the problem of proving the security of cryptographic systems. More significant, however, was the prestige that public-key cryptography got from being announced in the scientific world's most prominent lay journal more than six months before its appearance in the *Communications of the ACM*.

The excitement public-key cryptosystems provoked in the popular and scientific press was not matched by corresponding acceptance in the cryptographic establishment, however. In the same year that public-key cryptography was discovered, the National Bureau of Standards, with the support of the National Security Agency, proposed a conventional cryptographic system, designed by IBM, as a federal *Data Encryption Standard* [44]. Hellman and I criticized the proposal on the grounds that its key was too small

[37], but manufacturers were gearing up to support the proposed standard and our criticism was seen by many as an attempt to disrupt the standards-making process to the advantage of our own work. Public key in its turn was attacked, in sales literature [74] and technical papers [75, 59] alike, more as though it were a competing product than a recent research discovery. This, however, did not deter NSA from claiming its share of the credit. Its director, in the words of the *Encyclopaedia Britannica* [110], "pointed out that two-key cryptography had been discovered at the agency a decade earlier," though no evidence for this claim was ever offered publicly.

Far from hurting public key, the attacks and counterclaims added to a ground swell of publicity that spread its reputation far faster than publication in scientific journals alone ever could. The criticism nonetheless bears careful examination, because the field has been affected as much by discoveries about how public key cryptosystems should be used as by discoveries about how they can be built.

In viewing public-key cryptography as a new form of cryptosystem rather than a new form of key management, I set the stage for criticism on grounds of both security and performance. Opponents were quick to point out that the RSA system ran about one thousandth as fast as DES and required keys about ten times as large. Although it had been obvious from the beginning that the use of public-key systems could be limited to exchanging keys for conventional cryptography, it was not immediately clear that this was necessary. In this context, the proposal to build *hybrid* systems [62] was hailed as a discovery in its own right.

At present, the convenient features of public-key cryptosystems are bought at the expense of speed. The fastest RSA implementations run at only a few thousand bits per second, while the fastest DES implementations run at many million. It is generally desirable, therefore, to make use of a hybrid in which the public-key systems are used only during key management processes to establish shared keys for employment with conventional systems.

No known theorem, however, says that a public-key cryptosystem must be larger and slower than a conventional one. The demonstrable restrictions mandate a larger minimum block size (though perhaps no larger than that of DES) and preclude use in stream modes whose chunks are smaller than this minimum. For a long time I felt that "high-efficiency" public-key systems would be discovered and would supplant both current public key and conventional systems in most applications. Using public-key systems throughout, I argued, would yield a more uniform architecture with fewer components and would give the best possible damage limitation in the event of a key distribution center compromise [38]. Most important, I thought, if only one system were in use, only one certification study would be required. As certification is the most fundamental and most difficult problem in cryptography, this seemed to be where the real savings lay.

In time I saw the folly of this view. Theorems or not, it seemed silly to expect that adding a major new criterion to the requirements for a cryptographic system could fail to slow it down. The designer would always have more latitude with systems that did not have to satisfy the public key property and some of these would doubtless be faster. Even more compelling was the realization that modes of operation incompatible with the public-key property are essential in many communication channels.

To do
had hop
lic-key
applica
mental
makes
this cri
key dis

Key M:

The
conver
key di:
that sh
bootst
scribe
munic
to obt
sation

Key
cost o
conne
clock:
itate,
lowin
prope
sage a
will fa
rity in
oppo
text,
authent
conce

1)

2)

3)

4)

Ali
on e'
use.
ing t
num
disti
secu
men
the s
if it
A
mad
func
Alic.
Bob

DIFF

To date, the "high-efficiency public-key systems" that I had hoped for have not appeared and the restriction of public-key cryptography to key management and signature applications is almost universally accepted. More fundamental criticism focuses on whether public-key actually makes any contribution to security, but, before examining this criticism, we must undertake a more careful study of key distribution mechanisms.

Key Management

The solution to the problem of key management using conventional cryptography is for the network to provide a *key distribution center (KDC)*: a trusted network resource that shares a key with each subscriber and uses these in a bootstrap process to provide additional keys to the subscribers as needed. When one subscriber wants to communicate securely with another, he first contacts the KDC to obtain a *session key* for use in that particular conversation.

Key distribution protocols vary widely depending on the cost of messages, the availability of multiple simultaneous connections, whether the subscribers have synchronized clocks, and whether the KDC has authority not only to facilitate, but to allow or prohibit, communications. The following example is typical and makes use of an important property of cryptographic authentication. Because a message altered by anyone who does not have the correct key will fail when tested for authenticity, there is no loss of security in receiving a message from the hands of a potential opponent. In so doing, it introduces, in a conventional context, the concept of a *certificate*—a cryptographically authenticated message containing a cryptographic key—a concept that plays a vital role in modern key management.

- 1) When Alice wants to call Bob, she first calls the KDC and requests a key for communicating with Bob.
- 2) The KDC responds by sending Alice a pair of certificates. Each contains a copy of the required session key, one encrypted so that only Alice can read it and one so that only Bob can read it.
- 3) When Alice calls Bob, she presents the proper certificate as her introduction. Each of them decrypts the appropriate certificate under the key that he shares with the KDC and thereby gets access to the session key.
- 4) Alice and Bob can now communicate securely using the session key.

Alice and Bob need not go through all of this procedure on every call; they can instead save the certificates for later use. Such *cacheing* of keys allows subscribers to avoid calling the KDC every time they pick up the phone, but the number of KDC calls is still proportional to the number of distinct pairs of subscribers who want to communicate securely. A far more serious disadvantage of the arrangement described above is that the subscribers must share the secrecy of their keying information with the KDC and if it is penetrated, they too will be compromised.

A big improvement in both economy and security can be made by the use of public-key cryptography. A certificate functions as a letter of introduction. In the protocol above, Alice has obtained a letter that introduces her to Bob and Bob alone. In a network using public-key encryption, she

can instead obtain a single certificate that introduces her to any network subscriber [62].

What accounts for the difference? In a conventional network, every subscriber shares a secret key with the KDC and can only authenticate messages explicitly meant for him. If one subscriber has the key needed to authenticate a message meant for another subscriber, he will also be able to create such a message and authentication fails. In a public-key network, each subscriber has the public key of the KDC and thus the capacity to authenticate any message from the KDC, but no power to forge one.

Alice and Bob, each having obtained a certificate from the KDC in advance of making any secure calls, communicate with each other as follows:

- 1) Alice sends her certificate to Bob.
- 2) Bob sends his certificate to Alice.
- 3) Alice and Bob each check the KDC's signature on the certificates they have received.
- 4) Alice and Bob can now communicate using the keys contained in the certificates.

When making a call, there is no need to call the KDC and little to be gained by cacheing the certificates. The added security arises from the fact that the KDC is not privy to any information that would enable it to spy on the subscribers. The keys that the KDC dispenses are public keys and messages encrypted with these can only be decrypted by using the corresponding secret keys, to which the KDC has no access.

The most carefully articulated attack came from Roger Needham and Michael Schroeder [76], who compared conventional key distribution protocols with similar public-key ones. They counted the numbers of messages required and concluded that conventional cryptography was more efficient than public-key cryptography. Unfortunately, in this analysis, they had ignored the fact that security was better under the public-key protocol they presented than the conventional one.

In order to compromise a network that employs conventional cryptography, it suffices to corrupt the KDC. This gives the intruders access to information sufficient for recovering the session keys used to encrypt past, present, and perhaps future messages. These keys, together with information obtained from passive wiretaps, allow the penetrators of the KDC access to the contents of any message sent on the system.

A public-key network presents the intruder with a much more difficult problem. Even if the KDC has been corrupted and its secret key is known to opponents, this information is insufficient to read the traffic recorded by a passive wiretap. The KDC's secret key is useful only for signing certificates containing subscribers' public keys; it does not enable the intruders to decrypt any subscriber traffic. To be able to gain access to this traffic, the intruders must use their ability to forge certificates as a way of tricking subscribers into encrypting messages with phony public keys.

In order to spy on a call from Alice to Bob, opponents who have discovered the secret key of the KDC must intercept the message in which Alice sends Bob the certificate for her public key and substitute one for a public key they have manufactured themselves and whose corresponding secret key is therefore known to them. This will enable them to decrypt any message that Alice sends to Bob. If such a mis-

encrypted message actually reach Bob, however, he will be unable to decrypt it and may alert Alice to the error. The opponents must therefore intercept Alice's messages, decrypt them, and reencrypt them in Bob's public key in order to maintain the deception. If the opponents want to understand Bob's replies to Alice, they must go through the same procedure with Bob, supplying him with a phony public key for Alice and translating all the messages he sends her.

The procedure above is cumbersome at best. Active wiretaps are in principle detectable, and the number the intruders must place in the net in order to maintain their control, grows rapidly with the number of subscribers being spied on. Over large portions of many networks—radio broadcast networks, for example—the message deletions essential to this scheme are extremely difficult. This forces the opponents to place their taps very close to the targets and recreates the circumstances of conventional wiretapping, thereby denying the opponents precisely those advantages of communications intelligence that make it so attractive.

It is worth observing that the use of a hybrid scheme diminishes the gain in security a little because the intruder does not need to control the channel after the session key has been selected. This threat, however, can be countered, without losing the advantages of a session key, by periodically (and unpredictably) using the public keys to exchange new session keys [40].

Public-key techniques also make it possible to conquer another troubling problem of conventional cryptographic security, the fact that compromised keys can be used to read traffic taken at an earlier date. At the trial of Jerry Whitworth, a spy who passed U.S. Navy keying information to the Russians, the judge asked the prosecution's expert witness [27]: "Why is it necessary to destroy yesterday's . . . [key] . . . list if it's never going to be used again?" The witness responded in shock: "A used key, Your Honor, is the most critical key there is. If anyone can gain access to that, they can read your communications."

The solution to this problem is to be found in a judicious combination of exponential key exchange and digital signatures, inherent in the operation of a secure telephone currently under development at Bell-Northern Research [41], [81] and intended for use on the Integrated Services Digital Network.

Each ISDN secure phone has an operating secret-key/public-key pair that has been negotiated with the network's key management facility. The public-key portion is embodied in a certificate signed by the key management facility along with such identifying information as its phone number and location. In the call setup process that follows, the phone uses this certificate to convey its public key to other phones.

- 1) The telephones perform an exponential key exchange to generate session keys unique to the current phone call. These keys are then used to encrypt all subsequent transmissions in a conventional cryptosystem.
- 2) Having established an encrypted (though not yet authenticated) channel, the phones begin exchanging credentials. Each sends the other its public-key certificate.
- 3) Each phone checks the signature on the certificate it

has received and extracts from it the other phone's public key.

- 4) The phones now challenge each other to sign test messages and check the signatures on the responses using the public keys from the certificates.

Once the call setup is complete, each phone displays for its user the identity of the phone with which it is in communication.

The use of the exponential key exchange creates unique session keys that exist only inside the phones and only for the duration of the call. This provides a security guarantee whose absence in conventional cryptography is at the heart of many spy cases: once a call between uncompromised ISDN secure phones is completed and the session keys are destroyed, no compromise of the long term keys that still reside in the phones will enable anyone to decrypt the recording of the call. Using conventional key management techniques, session keys are always derivable from a combination of long-term keying material and intercepted traffic. If long-term conventional keys are ever compromised, all communications, even those of earlier date, encrypted in derived keys, are compromised as well.

In the late 1970s, a code clerk named Christopher Boyce, who worked for a CIA-sponsored division of TRW, copied keying material that was supposed to have been destroyed and sold it to the Russians [66]. More recently, Jerry Whitworth did much the same thing in the communication center of the Alameda Naval Air Station [8]. The use of exponential key exchange would have rendered such previously used keys virtually worthless.

Another valuable ingredient of modern public-key technology is the *message digest*. Implementing a digital signature by encrypting the entire document to be signed with a secret key has two disadvantages. Because public key systems are slow, both the signature process (encrypting the message with a secret key), and the verification process (decrypting the message with a public key) are slow. There is also another difficulty. If the signature process encrypts the entire message, the recipient must retain the ciphertext for however long the signed message is needed. In order to make any use of it during this period, he must either save a plaintext copy as well or repeatedly decrypt the ciphertext.

The solution to this problem seems first to have been proposed by Donald Davies and Wyn Price of the National Physical Laboratory in Teddington, England. They proposed constructing a cryptographically compressed form or digest of the message [33] and signing by encrypting this with the secret key. In addition to its economies, this has the advantage of allowing the signature to be passed around independently of the message. This is often valuable in protocols in which a portion of the message that is required in the authentication process is not actually transmitted because it is already known to both parties.

Most criticism of public-key cryptography came about because public-key management has not always been seen from the clear, certificate oriented, view described above. When we first wrote about public key, we spoke either of users looking in a public directory to find each other's keys or simply of exchanging them in the course of communication. The essential fact that each user had to authenticate any public key he received was glossed over. Those with

an inv
point
matize
proble
cism i

VIII.

Whi
tograd
one pe
of the
ratorie
aspect
nature
limite:
order l
one to
tion of
a nucle
the info
to deve
[89] and
[16], [3-

The
quenth
tories [section
to Verit
States a
other's
each of
fifty kil
testing
be tigh
one kil
assure
tamper
Conver
solve th
nation
monito
packag
weapon
remote
cannot

Digit
signed i
be alter
can ass
authorit
a nearby
of the tr

The R
applicat
out the
implem
cation [and high
Sandi
colleagu
tists, lea
approxii

an investment in traditional cryptography were not slow to point out this oversight. Public-key cryptography was stigmatized as being weak on authentication and, although the problems the critics saw have long been solved, the criticism is heard to this day.

VIII. APPLICATION AND IMPLEMENTATION

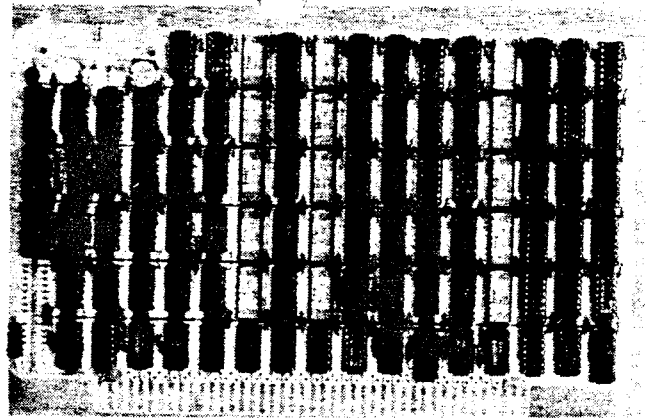
While arguments about the true worth of public-key cryptography raged in the late 1970s, it came to the attention of one person who had no doubt: Gustavus J. Simmons, head of the mathematics department of Sandia National Laboratories. Simmons was responsible for the mathematical aspects of nuclear command and control and digital signatures were just what he needed. The applications were limitless: A nuclear weapon could demand a digitally signed order before it would arm itself; a badge admitting someone to a sensitive area could bear a digitally signed description of the person; a sensor monitoring compliance with a nuclear test ban treaty could place a digital signature on the information it reported. Sandia began immediately both to develop the technology of public-key devices [108], [107], [89] and to study the strength of the proposed systems [105], [16], [34].

The application about which Simmons spoke most frequently, test-ban monitoring by remote seismic observatories [106], is the subject of another paper in this special section (G. J. Simmons, "How to Insure that Data Acquired to Verify Treaty Compliance are Trustworthy"). If the United States and the Soviet Union could put seismometers on each other's territories and use these seismometers to monitor each other's nuclear tests, the rather generous hundred and fifty kiloton upper limit imposed on underground nuclear testing by the Limited Nuclear Test Ban Treaty of 1963 could be tightened considerably—perhaps to ten kilotons or even one kiloton. The problem is this: A monitoring nation must assure itself that the host nation is not concealing tests by tampering with the data from the monitor's observatories. Conventional cryptographic authentication techniques can solve this problem, but in the process create another. A host nation wants to assure itself that the monitoring nation can monitor only total yield and does not employ an instrument package capable of detecting staging or other aspects of the weapon not covered by the treaty. If the data from the remote seismic observatory are encrypted, the host country cannot tell what they contain.

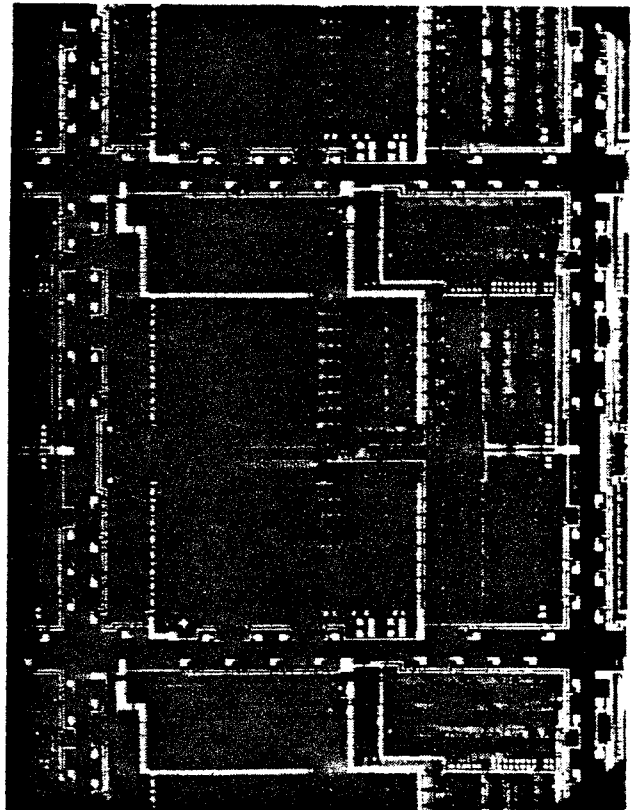
Digital signatures provided a perfect solution. A digitally signed message from a remote seismic observatory cannot be altered by the host, but can be read. The host country can assure itself that the observatory is not exceeding its authority by comparing the data transmitted with data from a nearby observatory conforming to its own interpretation of the treaty language.

The RSA system was the one best suited to signature applications, so Sandia began building hardware to carry out the RSA calculations. In 1979 it announced a board implementation intended for the seismic monitoring application [106]. This was later followed by work on both low- and high-speed chips [89], [94].

Sandia was not the only hardware builder. Ron Rivest and colleagues at MIT, ostensibly theoretical computer scientists, learned to design hardware and produced a board at approximately the same time as Sandia. The MIT board



Sandia 256-bit RSA board.



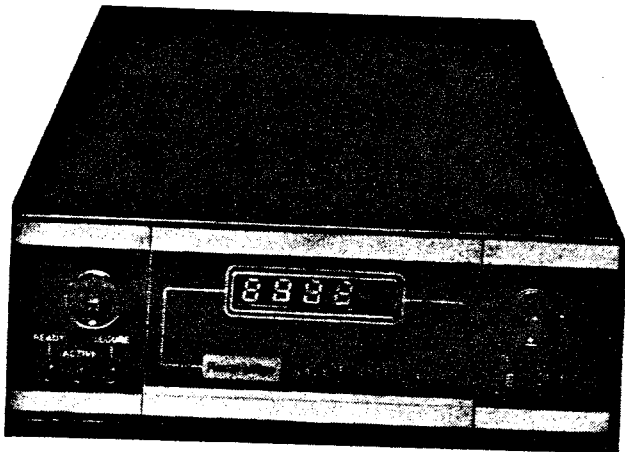
Wafer photo: Sandia low speed chip.

would carry out an RSA encryption with a one hundred digit modulus in about a twentieth of a second. It was adequate "proof of concept" but too expensive for the commercial applications Rivest had in mind.

No sooner was the board done than Rivest started studying the recently popularized methods for designing large-scale integrated circuits. The result was an experimental nMOS chip that operated on approximately 500 bit numbers and should have been capable of about three encryptions per second [93]. This chip was originally intended as a prototype for commercial applications. As it happened, the chip was never gotten to work correctly, and the appearance of a commercially available RSA chip was to await the brilliant work of Cylink corporation in the mid-1980s [31].

As the present decade dawned, public-key technology began the transition from esoteric research to product development. Part of AT&T's response (Carter Administration initiative to improve the overall security of American telecommunications, was to develop a specialized cryptographic device for protecting the Common Channel Interoffice Signaling (CCIS) on telephone trunks. The devices were link encryptors that used exponential key exchange to distribute DES keys [75], [16].

Although AT&T's system was widely used within its own huge network, it was never made available as a commercial product. At about the same time, however, Racal-Milgo began producing the Datacryptor II, a link encryption device that offered an RSA key exchange mode [87]. One



Racal-Milgo Datacryptor II.

device used exponential key exchange, the other RSA, but overall function was quite similar. When the public-key option of the Datacryptor is initialized, it manufactures a new RSA key pair and communicates the public portion to the Datacryptor at the other end of the line. The device that receives this public key manufactures a DES key and sends it to the first Datacryptor encrypted with RSA. Unfortunately, the opportunity for sophisticated digital signature based authentication that RSA makes possible was missed.

Future Secure Voice System

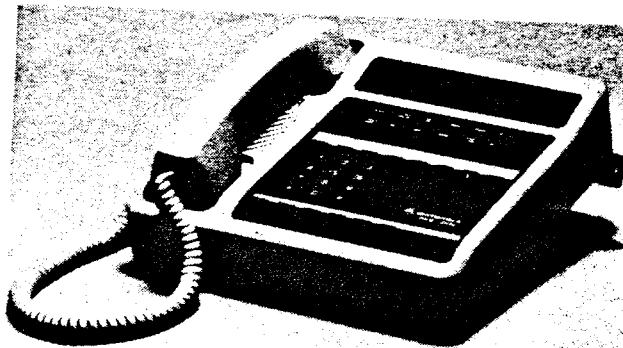
As the early 1980s became the mid-1980s, public-key cryptography finally achieved official, if nominally secret, acceptance. In 1983, NSA began feasibility studies for a new secure phone system. There was fewer than ten-thousand of their then latest system the Secure Telephone Unit II or STU-II and already the key distribution center for the principal network was overloaded, with users often complaining of busy signals. At \$12 000 or more apiece, ten-thousand STU-IIs may have been all the government could afford, but it was hardly all the secure phones that were needed. In its desire to protect far more than just explicitly classified communications, NSA was dreaming of a million phones, each able to talk to any of the others. They could not have them all calling the key distribution center every day.

The system to be replaced employed electronic key distribution that allowed the STU-II to bootstrap itself into direct end-to-end encryption with a different key on every call. When a STU-II made a secure call to a terminal with

which it did not share a key, it acquired one by calling a key distribution center using a protocol similar to one described earlier.

Although the STU-II seemed wonderful when first fielded in the late seventies, it had some major shortcomings. Some caching of keys was permitted, but calls to the KDC entailed significant overhead. Worse, each network had to be at a single clearance level, because there was no way for a STU-II to inform the user of the clearance level of the phone with which it was talking. These factors, as much as the high price and large size, conspired against the feasibility of building a really large STU-II network.

The STU-III is the size of a large conventional telephone and, at about \$3000 apiece, substantially cheaper than its predecessor. It is equipped with a two-line display that, like the display of the ISDN secure phone, provides information to each party about the location, affiliation, and clearance of the other. This allows one phone to be used for the protection of information at various security levels. The phones are also sufficiently tamper resistant that unlike earlier



Motorola STU-III secure telephone.

equipment, the unkeyed instrument is unclassified. These elements will permit the new system to be made much more widely available with projections of the number in use by the early 1990s running from half a million to three million [18], [43].

To make a secure call with a STU-III, the caller first places an ordinary call to another STU-III, then inserts a key-shaped device containing a cryptographic variable and pushes a "go secure" button. After an approximately fifteen second wait for cryptographic setup, each phone shows information about the identity and clearance of the other party on its display and the call can proceed.

In an unprecedented move, Walter Deeley, NSA's deputy director for communications security, announced the STU-III or Future Secure Voice System in an exclusive interview given to *The New York Times* [18]. The objective of the new system was primarily to provide secure voice and low-speed data communications for the U.S. Defense Department and its contractors. The interview did not say much about how it was going to work, but gradually the word began to leak out. The new system was using public key.

The new approach to key management was reported early on [88] and one article [6] spoke of phones being "reprogrammed once a year by secure telephone link," a turn of phrase strongly suggestive of a certificate passing protocol, similar to that described earlier, that minimizes the need for phones to talk to the key management center. Recent

reports ha
managem
public key
traffic enc
monysub
suggest a c
ilar to that
that FIREFI

Three co
facturing tl
is building
have been
began in N

Current Co

Several
technolog
establishe
exploit the

The first
Shamir, ar
tem, to ex
based on t
software p
ing electri
tem availa
that has be

Cylink C
up the mo
keyfield. It
speed (1.5



Cylink CIDI

phone tru
nential ke

Cylink i
RSA chip



Cylink CY11

in time, proportional to

$$L(n) = e^{\sqrt{\ln n \times \ln \ln n}}$$

a figure that has already been seen in connection with discrete logarithms. The one that has been most widely applied is called quadratic sieve factoring [34] and lends itself well to machine implementation. One of factoring's gurus, Marvin Wunderlich, gave a paper in 1983 [116] that examined the way in which quadratic sieve factoring could exploit parallel processing to factor a hundred digit number in two months. In the same lecture, Wunderlich also explained the importance of uniformity in factoring methods applied in cryptanalysis. To be used in attacking RSA, a factoring method must be uniform, at least over the class of bicomposite numbers. If it is only applicable to numbers of some particular form, as many methods used by number theorists have been, the cryptographers will simply alter their key production to avoid numbers of that form.

More recently, Carl Pomerance [85] has undertaken the design of a modular machine employing custom chips and specialized to factoring. The size of the numbers you can factor is dependent on how much of such a machine you can afford. He has begun building a \$25 000 implementation that he expects to factor 100 digit numbers in two weeks [96]. Ten million dollars worth of similar hardware would be able to factor hundred and fifty digit numbers in a year, but Pomerance's analysis does not stop there. Fixing one year as a nominal upper limit on our patience with factoring any one number, he is prepared to give a dollar estimate for factoring a number of any size. For a two hundred digit number, often considered unapproachable and a benchmark in judging RSA systems, the figure is one hundred billion dollars. This is a high price to be sure, but not beyond human grasp.

Prime Finding

Prime finding has followed a somewhat different course from factoring. This is in part because there are probabilistic techniques that identify primes with sufficient certainty to satisfy all but perhaps the pickiest of RSA users and in part because primality is not in itself a sufficient condition for numbers to be acceptable as RSA factors.

Fermat's Little Theorem guarantees that if n is prime then for all $0 < b < n$

$$b^{n-1} \equiv 1 \pmod{n}$$

and any number that exhibits this property for some b is said to pass the pseudoprime test to base b . Composite numbers that pass pseudoprime tests to all bases exist, but they are rare and a number that passes several pseudoprime tests is probably a prime.

The test can be refined by making use of the fact that if n is an odd prime only the numbers 1 and -1 are square roots of 1, whereas if n is the product of distinct odd primes, the number of square roots of unity grows exponentially in the number of factors. If the number n passes the pseudoprime test to base b , it can be further examined to see if

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}.$$

Tests of this kind are called strong pseudoprime tests to base b and very few composite numbers that pass strong pseudoprime tests to more than a few bases are known.

Although there has been intensive work in the past decade on giving genuine proofs of primality [84], [2], [51], the strong pseudoprime tests take care of the primality aspect of choosing the factors of RSA moduli. Another aspect arises from the fact that not all prime numbers are felt to be equally good. In many RSA implementations, the factors of the modulus are not random large primes p , but large primes chosen for particular properties of the factors of $p - 1$ [91], [52].

High-Speed Arithmetic

Because of the progress in factoring during the decade of public-key's existence, the size of the numbers used in RSA has grown steadily. In the early years, talk of hundred digit moduli was common. One hundred digit numbers, 332 bits, did not seem likely to be factored in the immediate future and, with the available computing techniques, systems with bigger moduli ran very slowly. Today, hundred digit numbers seem only just out of reach and there is little discussion of moduli smaller than 512 bits. Two hundred digits, 664 bits, is frequently mentioned, and Cylink has not only chosen to make its chip a comfortable 1028 bits, but also to allow up to sixteen chips to be used in cascade. If this expansion has been pushed by advances in factoring, it has been made possible by advances in arithmetic.

Most of the computation done both in encryption and decryption and in the ancillary activity of manufacturing keys is exponentiation and each exponentiation, in turn, is made up of multiplications. Because, as discussed in the section of exponential key exchange, numbers can be raised to powers in a small number of operations by repeated squaring, it is the speed of the underlying multiplication operation that is crucial.

According to Rivest [94] multiplication on a fixed word length processor takes time proportional to the square length of the operands or $O(k^2)$. If dedicated serial/parallel hardware is constructed for the purpose, this time can be reduced to $O(k)$. In this case, the number of gates required is also proportional to the lengths of the operands, $O(k)$. The fastest implementations [15] run in time $O(\log k)$, but here the hardware requirements grow sharply to $O(k^2)$ gates.

X. DIRECTIONS IN PUBLIC-KEY RESEARCH

Public-key cryptography has followed a curious course. In its first three years, three systems were invented. One was broken; one has generally been considered impractical; and the third reigns alone as the irreplaceable basis for a new technology. Progress in producing new public-key cryptosystems is stymied as is the complementary problem of proving the one system we have secure, or even of proving it equivalent to factoring in a useful way.

Stymied though it may be in its central problems, however, the theoretical side of public-key cryptography is flourishing. This is perhaps because the public-key problem changed the flavor of cryptography. It may be difficult to produce good conventional cryptosystems, but the difficulty is all below the surface. It is typically easier to construct a transformation that appears to satisfy the requirements of security than it is to show that a proposed system is not good. The result is a long development cycle ill-suited to the give and take of academic research. Systems that even

appear to exhibit difficult to find an theoretical computer science early taste of RSA has inspiringly paradoxical a variety of new

This is not to be motivated by applications cryptography in a mode of operation another. It is with block cryptosystems with which to proofs have chosen the system ifificational example is to be used. Cryptography has been such secondarily define the stream been made in protocols is and that the p

There is another of cryptographing our current in which communication. The digital signature, which can do with paper, be hard to do without them?

In 1977, I gave electronic alternative topics see Information Theoretic, arguing for of the problem mature. A year entitled "Ment of receipts for something just a way that pre being discovered.

To my delight covered in Berkeley problems that the emergence Crypto '82 [20]. either broken been sufficient tract signing, actual solutions.

In separate of Texas and Ad direction of in divided among them, but no secret sharing, full grown with

appear to exhibit the public-key property, however, are difficult to find and this sort of difficulty is something the theoretical computer scientists can get their teeth into. The early taste of success that came with the development of RSA has inspired the search for solutions to other seemingly paradoxical problems and led to active exploration of a variety of new cryptographic disciplines.

This is not to say that contemporary research is not motivated by application. A constant caution in conventional cryptography is that the strength of a cryptosystem in one mode of operation does not guarantee its strength in another. It is widely felt, for example, that a conventional block cryptosystem such as DES is a suitable component with which to implement other modes of operation, but no proofs have been offered. This burdens anyone who chooses the system as a building block with a separate certification examination of every configuration in which it is to be used. One objective of research in public-key cryptography has been to demonstrate the equivalence of many such secondary cryptographic problems to those that define the strength of the system. Substantial progress has been made in proving that the strength of cryptographic protocols is equivalent to the strength of the RSA system and that the protection provided by RSA is uniform [4].

There is another sort of applied flavor to even the purest of cryptographic research—a search for ways of transplanting our current social and business mechanisms to a world in which communication is primarily telecommunication. The digital signature was the first great success in this direction, which can be characterized as asking: What can we do with paper, pencil, coins, and handshakes that would be hard to do without them. And, how can we do it without them?

In 1977, I gave a talk on the problem of developing a purely electronic analog of the registered mail receipt, in the current topics session of the International Symposium on Information Theory at Cornell. My message was pessimistic, arguing for both the importance and the intractability of the problem, but fortunately my pessimism was premature. A year and a half later, the MIT group penned a note entitled "Mental Poker" [99]. It did not solve the problem of receipts for registered mail, but did show how to do something just as surprising: gamble over the telephone in a way that prevented either party from cheating without being discovered. This as it turned out was just the beginning.

To my delight, the problem of registered mail was rediscovered in Berkeley in 1982 as part of a larger category of problems that could be solved by ping-pong protocols and the emergence of this subject was one of the highlights of Crypto '82 [20]. Despite problems with protocols that were either broken or impossibly expensive [55], progress has been sufficient to provide hope that registered mail, contract signing, and related problems will one day have practical solutions.

In separate 1979 papers, G. R. Blakley at the University of Texas and Adi Shamir at MIT [11], [100] opened yet another direction of investigation: how secret information can be divided among several people in such a way that any k of them, but no fewer, can recover it. Although this field of secret sharing, unlike that of ping-pong protocols emerged full grown with provably correct and easily implementable

protocols, it has been the subject of continuing examination [5], [26], [45], [58].

David Chaum, currently at the Center for Mathematics and Computer Science in Amsterdam, has applied public-key technology to a particularly challenging set of problems [21], [22]. In a society dominated by telecommunication and computers, organizations ranging from credit bureaus to government agencies can build up dossiers on private citizens by comparing notes on the credentials issued to the citizens. This dossier building occurs without the citizens' knowledge or consent and, at present, the only protection against abuses of this power lies in legal regulation. Chaum has developed technical ways of permitting an individual to control the transfer of information about him from one organization to another. Without action on the part of an individual to whom credentials have been issued, no organization is able to link the information it holds about the individual with information in the databanks of any other organization. Nonetheless, the systems guarantee that no individual can forge organizational credentials. Chaum's techniques address problems as diverse as preventing spies from tracing messages through electronic mail networks [19], [24] and protecting the privacy of participants in transactions with systems that recapture in electronic media both the assurance and the anonymity of cash [21].

The work drawing most attention at present is probably the field best known under the name of zero-knowledge proofs [49], [50], though similar theories, based on different assumptions about the capabilities of the participants, have been developed independently [23], [13], [14]. One of the idea's originators, Silvio Micali at MIT, described it as "the inverse of a digital signature." A zero-knowledge proof permits Alice to demonstrate to Bob that she knows something, but gives him no way of conveying this assurance to anybody else. In the original example, Alice convinced Bob that she knew how to color a map with three colors, but gave him no information whatever about what the coloring was.

The view that a zero-knowledge proof is the inverse of a digital signature now seems ironic, because a form of challenge and response authentication, applicable to the signature problem, has become the best known outgrowth of the field. In this system, the responder demonstrates to the challenger his knowledge of a secret number, without revealing any information about what the number is. Amos Fiat and Adi Shamir have recently brought forth an identification system of this sort, and announced a proof that breaking it is equivalent to factoring [47].

A purist might respond to all this by saying that having failed to solve the real problems in public-key cryptography, cryptographers have turned aside to find other things about which to write papers. It is a situation that has been seen before in mathematics. At the end of the last century, mathematical analysis ground to a halt against intractable problems in Fourier Theory, differential equations, and complex analysis. What many mathematicians did with their time while not solving the great problems was viewed with scorn by critics who spoke of the development of point set topology and abstract algebra as "soft mathematics." Only at mid-century did it become clear what had happened. In the abstractions a great hammer had been forged and through the 1950s and 1960s the classic problems began to

fall under its blows. Perhaps cryptography will be equally lucky.

XI. WHERE IS PUBLIC KEY GOING?

In just over ten years, public-key cryptography has gone from a novel concept to a mainstay of cryptographic technology. It is soon to be implemented in hundreds of thousands of secure telephones and efforts are under way to apply the same mechanisms to data communications on a similar scale [97]. The outlook in the commercial world is equally bright. As early as the fourth quarter of this year, digital signatures may enter retail electronic funds transfer technology in a British experiment with point of sale terminals [57]. The demand for public key is exemplified by a recent conference on smart cards in Vienna, Austria [111], where one question was heard over and over again: When will we have an RSA card?

Now that it has achieved acceptance, public-key cryptography seems indispensable. In some ways, however, its technological base is disturbingly narrow. With the exception of the McEliece scheme and a cumbersome knapsack system devised explicitly to resist the known attacks [25], virtually all surviving public-key cryptosystems and most of the more numerous signature systems employ exponentiation over products of primes. They are thus vulnerable to breakthroughs in factoring or discrete logarithms. Key exchange systems are slightly better off since they can use the arithmetic of primes, prime products, or Galois fields with 2^n elements and are thus sensitive to progress on the discrete logarithm problem only.

From the standpoint of conventional cryptography, with its diversity of systems, the narrowness bespeaks a worrisome fragility. This worry, however, is mitigated by two factors.

- The operations on which public-key cryptography currently depends—multiplying, exponentiating, and factoring—are all fundamental arithmetic phenomena. They have been the subject of intense mathematical scrutiny for centuries and the increased attention that has resulted from their use in public-key cryptosystems has on balance enhanced rather than diminished our confidence.
- Our ability to carry out large arithmetic computations has grown steadily and now permits us to implement our systems with numbers sufficient in size to be vulnerable only to a dramatic breakthrough in factoring, logarithms, or root extraction.

It is even possible that RSA and exponential key exchange will be with us indefinitely. The fundamental nature of exponentiation makes both good candidates for eventual proof of security and if complexity theory evolves to provide convincing evidence of the strength of either, it will establish a new paradigm for judging cryptographic mechanisms. Even if new systems were faster and had smaller keys, the current systems might never be superseded altogether.

Such proofs have yet to be found, however, and proposed schemes are continually presented at the cryptographic conferences [12], [114], [80], [30], [82]. Approaches include generalizing RSA to other rings and various attempts to replace exponentials with polynomials, but in general they have not fared well and some of their fates are

discussed elsewhere in this special section (E. F. Brickell and A. M. Odlyzko "Cryptanalysis: A Survey of Recent Results"). So far, the goal of improving on the performance of RSA without decreasing its security has yet to be achieved.

An appealing idea that has been put forward by Stephen Wolfram and studied by Papua Guam [54] is the use of cellular automata. Guam's system is too new to have received careful scrutiny and superficial examination suggests that it may suffer a weakness similar to one seen in other cases [46]. Even should this effort fail, however, the cellular automaton approach is attractive. Cellular automata differ from such widely accepted cryptographic mechanisms as shift registers in that, even if they are invertible, it is not possible to calculate the predecessor of an arbitrary state by simply reversing the rule for finding the successor. This makes them a viable vehicle for trap doors. Cellular automata also lend themselves to study of the randomness properties required of strong cryptographic systems [115].

What will be the outcome of such research? In an attempt to foresee the future of cryptography in 1979, I wrote [39]:

"Prospects for development of new and more efficient public key cryptographic systems by the latter part of the eighties are quite good. Public key cryptography is more successful today than algebraic coding theory was at the age of four. The major breakthroughs in that field did not begin till the latter part of its first decade, but then progressed rapidly. The similarity of the two fields is reason for optimism that . . . public key cryptography will follow a similar course.

Increasing use of the available public key systems in the 1980s will spread awareness of both their advantages and the performance shortcomings of the early examples. The research response to this awareness will probably produce better public key systems in time for use during the first half of the nineties."

My schedule was clearly too optimistic. If there are public-key cryptosystems with better performance or greater security waiting in the wings, they are proprietary systems that have yet to make even their existence known. Other aspects of the argument are closer to the mark, however. The use of public-key cryptosystems has increased dramatically and with it awareness of their advantages. Judicious use of hybrid systems and improved arithmetic algorithms have reduced the "performance shortcomings" to the status of a nuisance in most applications and the biggest motivation for seeking new systems today is probably the desire not to have all our eggs in one basket. Unless the available systems suffer a cryptanalytic disaster, moreover, the very success of public-key cryptography will delay the introduction of new ones until the equipment now going into the field becomes outmoded for other reasons.

For a discipline just entering its teens, the position of public-key cryptography should be seen not as a fragile, but as a strong one.

REFERENCES

- [1] L. M. Adleman and R. L. Rivest, "How to break the Lu-Lee (COMSAT) public key cryptosystem," MIT Laboratory for Computer Science, July 24, 1979.

- [2] L. M. Adleman, C. Pomerance, and R. P. Rumley, "On distinguishing prime numbers from composite numbers," *Ann. Math.*, vol. 117, no. 2, pp. 173-206, 1983.
- [3] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*. Reading, MA: Addison-Wesley, 1974.
- [4] W. Alexi, B. Chor, O. Goldreich, and C. P. Schnor, "RSA/Rabin bits are $1/2 + 1/(\text{poly}(\log N))$ secure," in *25th Annual IEEE Symp. on Foundations of Comp. Sci.*, pp. 449-457, 1984.
- [5] C. Asmuth and J. Blum, "A modular approach to key safeguarding," *IEEE Trans. Informat. Theory*, vol. IT-29, pp. 208-210, Mar. 1983.
- [6] "Contractors ready low-cost, secure telephone for 1987 service start," *Aviat. Week Space Technol.*, pp. 114-115, Jan. 1986.
- [7] C. Barney, "Cypher chip makes key distribution a snap," *Electronics*, Aug. 7, 1986.
- [8] J. Barron, *Breaking the Ring*. Boston, MA: Houghton Mifflin, 1987.
- [9] D. ben-Aaron, "Mailsafe signs, seals, and delivers files," *Information Week*, pp. 19-22, Sept. 15, 1986.
- [10] I. F. Blake, R. Fuji-Hara, R. C. Mullin, and S. A. Vanstone, "Computing logarithms in finite fields of characteristic two," *SIAM J. Alg. Disc. Methods*, vol. 5, no. 2, pp. 276-285, June 1984.
- [11] G. R. Blakley, "Safeguarding cryptographic keys," in *National Computer Conf.*, pp. 313-317, 1979.
- [12] G. R. Blakley and D. Chaum, Eds., *Advances in Cryptology: Proceedings of Crypto '84*. Berlin, Germany: Springer-Verlag, 1985.
- [13] G. Brassard and C. Crépeau, "Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond," in *27th Annual IEEE Symp. on the Foundations of Comp. Sci.*, pp. 188-195, 1986.
- [14] G. Brassard, C. Crépeau, and D. Chaum, "Minimum disclosure proofs of disclosure proofs of knowledge," Center for Mathematics and Computer Science, Amsterdam, Rep. PM-R8710, Dec. 1987. (To appear as an invited paper in *J. Comput. Syst. Sci.*)
- [15] E. F. Brickell, "A fast modular multiplication algorithm with application to two key cryptography," in *Crypto '82* [20], pp. 51-60.
- [16] E. F. Brickell and G. J. Simmons, "A status report on knapsack based public key cryptosystems," *Congressus Numerantium*, vol. 7, pp. 3-72, 1983. The CCIS encryptor is mentioned on pp. 4-5.
- [17] E. F. Brickell, "Breaking iterated knapsacks," in *Crypto '84* [12], pp. 342-358.
- [18] D. Burnham, "NSA seeking 500,000 'secure' telephones," *The New York Times*, October 7, 1984.
- [19] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *CACM*, vol. 24, no. 2, pp. 84-88, Feb. 1981.
- [20] D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., *Advances in Cryptology, Proceedings of Crypto '82*. New York, NY: Plenum, 1983.
- [21] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *CACM*, vol. 28, no. 10, pp. 1030-1044, Oct. 1985.
- [22] D. Chaum and J.-H. Evertse, "A secure and privacy-protecting protocol for transmitting personal information between organizations," in *Crypto '86* [80], pp. 118-167.
- [23] D. Chaum, "Demonstrating that a public predicate can be satisfied without revealing any information about how," in *Crypto '86* [80], pp. 195-199.
- [24] —, "The dining cryptographers problem: Unconditional sender untraceability," *J. Cryptology*, vol. 1, no. 1, pp. 65-75, 1988.
- [25] B. Chor and R. L. Rivest, "A knapsack type public-key cryptosystem based on arithmetic in finite fields," in *Crypto '84* [12], pp. 54-65.
- [26] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *26th Annual IEEE Symp. on the Foundations of Comp. Sci.*, pp. 383-395, 1985.
- [27] Testimony of David Earl Clark at the trial of Jerry Alfred Whitworth before Judge J. P. Vukasin, Jr., in the U.S. District Court, Northern District of California, Mar. 25, 1986. Reported by Viviana Balboni, pp. 11-1345.
- [28] D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two," *IEEE Trans. Informat. Theory*, vol. IT-30, pp. 587-594, 1984.
- [29] D. Coppersmith, A. M. Odlyzko, and R. Schroepel, "Discrete logarithms in $GF(p)$," *Algorithmica*, vol. 1, pp. 1-16, 1986.
- [30] N. Cot and I. Ingemarsson, Eds., *Advances in Cryptology, Proceedings of EUROCRYPT '84*. Berlin, Germany: Springer-Verlag, 1985.
- [31] "Cidec-HS high speed DES encryption for digital networks," product description, Cylink Corporation, Sunnyvale, CA.
- [32] "Key management development package," product description, Cylink Corporation, Sunnyvale, CA.
- [33] D. W. Davies and W. L. Price, "The applications of digital signatures based on public key cryptosystems," National Physical Laboratory Rep. DNACS 39/80, Dec. 1980.
- [34] J. A. Davis, D. B. Holdridge, and G. J. Simmons, "Status report on factoring (at the Sandia National Laboratories)," in *Eurocrypt '84* [30], pp. 183-215.
- [35] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," in *Proc. Nat. Computer Conf.*, (New York, NY), pp. 109-112, June 7-10, 1976.
- [36] —, "New directions in cryptography," *IEEE Trans. Informat. Theory*, vol. IT-22, pp. 644-654, Nov. 1976.
- [37] —, "Exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, vol. 10, no. 6, pp. 74-84, June 1977.
- [38] W. Diffie, "Conventional versus public key cryptosystems," in [109], pp. 41-72. Rabin's system is discussed on p. 70, the relative strength of conventional and public-key distribution on pp. 64-66.
- [39] —, "Cryptographic technology: Fifteen-year forecast," in [109], pp. 301-327.
- [40] —, "Securing the DoD transmission control protocol," in *Crypto '85* [114], pp. 108-127.
- [41] W. Diffie, L. Strawczynski, B. O'Higgins, and D. Steer, "An ISDN secure telephone unit," in *Proc. National Communications Forum 1987*, pp. 473-477.
- [42] E. Dolnick, "N.M. scientist cracks code, wins \$1000," *The Boston Globe*, Nov. 6, 1984.
- [43] Electronic Industries Association, "Comsec and Compusec market study," Jan. 14, 1987.
- [44] Federal Register, "Encryption algorithm for computer data protection," vol. 40, no. 52, pp. 12134-12139, Mar. 17, 1975.
- [45] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *28th Annual IEEE Symp. on the Foundations of Comp. Sci.*, pp. 427-437, 1987.
- [46] H. Fell and W. Diffie, "Analysis of a public key approach based on polynomial substitution," in *Crypto '85* [114], pp. 108-127.
- [47] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Crypto '86* [80], pp. 186-212.
- [48] M. Gardner, "A new kind of cipher that would take millions of years to break," *Sci. Amer.*, pp. 120-124 (Mathematical Games), Aug. 1977.
- [49] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design," in *27th Annual IEEE Conf. on the Foundations of Comp. Sci.*, pp. 174-187, 1986.
- [50] S. Goldwasser, S. Micali, and C. Rackoff, "Knowledge complexity of interactive proofs," in *17th Symp. on the Theory of Computing*, pp. 291-304, 1985.
- [51] S. Goldwasser and J. Killian, "All primes can be quickly certified," in *18th Symp. on the Theory of Computing*, pp. 316-329, 1986.
- [52] J. Gordon, "Strong primes are easy to find," in *Eurocrypt '84* [30], pp. 215-223.
- [53] —, speech at the Zurich Seminar, 1984. In this lecture, which has unfortunately never been published, Gordon assembled the facts of Alice and Bob's precarious lives, which had previously been available only as scattered references in the literature.
- [54] P. Guam, "Cellular automaton public key cryptosystem," *Complex Systems*, vol. 1, pp. 51-56, 1987.
- [55] J. Hastad and A. Shamir, "The cryptographic security of trunc-

- lated linearly related "tables," in *17th Symp. on Theory of Computing*, pp. 356-361, 1985.
- [56] D. Helwig, "Coding chip devised in Waterloo," *The Globe and Mail*, Jan. 1, 1987.
- [57] "National EFT POS to use public key cryptography," *Information Security Monitor*, vol. 2, no. 12, p. 1, Nov. 1987.
- [58] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Globecom '87*, pp. 361-364, 1987.
- [59] C. S. Kline and G. J. Popek, "Public key vs. conventional key encryption," in *National Computer Conf.*, 1979.
- [60] D. Knuth, "Semi-numerical algorithms," in *The Art of Computer Programming*, vol. 2, 2nd ed. Reading, MA: Addison-Wesley, 1981, pp. 316-336.
- [61] N. Koblitz, *A Course in Number Theory and Cryptography*. New York, NY: Springer-Verlag, 1987.
- [62] L. M. Kohnfelder, "Toward a practical public key cryptosystem," Bachelors Thesis, MIT Dept. of Electrical Engineering, May 1978.
- [63] R. Kopeck, "T1 encryption plan protects data," *PC Week*, March 3, 1987.
- [64] J. Kowalchuk, B. P. Schanning, and S. Powers, "Communication privacy: Integration of public and secret key cryptography," in *National Telecommunications Conf.*, (Houston, TX), pp. 49.1.1-5, Nov. 30-Dec. 4, 1980.
- [65] E. Kranakis, *Primality and Cryptography*. New York, NY: Wiley, 1986.
- [66] R. Lindsey, *The Falcon and the Snowman*. New York, NY: Simon and Schuster, 1979.
- [67] S. Lu and L. Lee, "A simple and effective public key cryptosystem," *Comsat Technical Rev.*, vol. 9, no. 1, Spring 1979.
- [68] K. S. McCurley, "A key distribution system equivalent to factoring," Department of Mathematics, University of Southern California, June 3, 1987.
- [69] R. J. McEliece, "A public key cryptosystem based on algebraic coding theory," *JPL DSN Progress Rep.* 42-44, pp. 114-116, Jan.-Feb. 1978.
- [70] R. Merkle, "Secure communication over insecure channels," *CACM*, pp. 294-299, Apr. 1978.
- [71] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trap door knapsacks," *IEEE Trans. Informat. Theory*, vol. IT-24, pp. 525-30, Sept. 1978.
- [72] R. Merkle, Letters to the Editor, *Time Magazine*, vol. 120, no. 20, p. 8, Nov. 15, 1982.
- [73] M. A. Morrison and J. Brillhart, "A method of factoring and the factorization of F_7 ," *Math. Comp.*, vol. 29, pp. 18-205, 1975.
- [74] "Advanced techniques in network security," Motorola Government Electronics Division, Scottsdale, AZ, about 1977.
- [75] F. H. Myers, "A data link encryption system," in *National Telecommunications Conf.*, (Washington, DC), pp. 4.5.1-4.5.8, Nov. 27-29, 1979.
- [76] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *CACM*, vol. 21, pp. 993-999, Dec. 1978.
- [77] L. Neuwirth, "A comparison of four key distribution methods," *Telecommunications*, pp. 110-111, 114-115, July 1986.
- [78] "Statement of Lee Neuwirth of Cylink on HR145," submitted to Congressional committees considering HR145, Feb. 1987.
- [79] A. M. Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," in *Eurocrypt '84* [30], pp. 225-314.
- [80] —, Ed., *Advances in Cryptology-CRYPTO '86*. Berlin, Germany: Springer-Verlag, 1987.
- [81] B. O'Higgins, W. Diffie, L. Strawczynski, and R. de Hoog, "Encryption and ISDN-A natural fit," in *International Switching Symp.*, (Phoenix, AZ), pp. A11.4.1-7, Mar. 16-20, 1987.
- [82] F. Pichler, Ed., *Advances in Cryptology-Proceedings of EUROCRYPT '85*. Berlin, Germany: Springer-Verlag, 1986.
- [83] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms in $GF(p)$ and its cryptographic significance," *IEEE Trans. Informat. Theory*, vol. IT-24, pp. 106-110, Jan. 1978.
- [84] C. Pomerance, "Recent developments in primality testing," *The Mathematical Intelligence*, vol. 3, no. 3, pp. 97-105, 1981.
- [85] C. Pomerance, J. W. Smith, and R. Tuler, "A pipe-line architecture for factoring large integers with the quadratic sieve algorithm," to appear in a special issue on cryptography of the *SIAM J. Computing*.
- [86] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," *MIT Laboratory for Computer Science, MIT/LCS/TR-212*, Jan. 1979.
- [87] "Datacryptor II, public key management option," *Each Milgo*, Sunrise Florida, 1981.
- [88] "AT&T readying new spy-proof phone for big military and civilian markets," *The Report on AT&T*, pp. 6-7, June 2, 1987.
- [89] R. F. Riedel, J. B. Snyder, R. J. Widman, and W. J. Barnard, "A two-chip implementation of the RSA public-key encryption algorithm," in *GOMAC (Government Microcircuit Applications Conference)*, (Orlando, FL), pp. 24-27, Nov. 1982.
- [90] R. L. Rivest, A. Shamir, and L. Adleman, "On digital signatures and public key cryptosystems," *MIT Laboratory for Computer Science, MIT/LCS/TR-212*, Jan. 1979.
- [91] —, "A method for obtaining digital signatures and public key cryptosystems," *CACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.
- [92] R. Rivest, personal communication with H. C. Williams cited on p. 729 in [113].
- [93] —, "A description of a single-chip implementation of the RSA cipher," *Lambda*, vol. 1, no. 3, pp. 14-18, Fall 1980.
- [94] —, "RSA chips (past/present/future)," in *Eurocrypt '84* [30], pp. 159-165.
- [95] H. L. Rogers, "An overview of the caneware program," paper 31, presented at the 3rd Annual Symp. on Physical/Electronic Security, Armed Forces Communications and Electronics Association, Philadelphia Chapter, Aug. 1987.
- [96] "Toward a new factoring record," *Science News*, p. 62, Jan. 23, 1987.
- [97] "SDNS: A network on implementation," in *10th National Computer Security Conf.*, (Baltimore, MD), pp. 150-174, Sept. 21-24, 1987. Session containing six papers on the Secure Data Network System.
- [98] A. Shamir, "A fast signature scheme," M.I.T. Laboratory for Computer Science, Technical Memorandum, MIT/LCS/TM-107, July 1978.
- [99] A. Shamir, R. L. Rivest, and L. M. Adleman, "Mental poker," MIT Laboratory for Computer Science, Technical Memorandum, MIT/LCS/TM-125, Jan. 29, 1979.
- [100] A. Shamir, "How to share a secret," *CACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.
- [101] —, "A polynomial-time algorithm for breaking Merkle-Hellman cryptosystems (extended abstract)," Research announcement, preliminary draft, Applied Mathematics, Weizmann Institute, Rehovot, Israel, April 20, 1982. This paper appeared with a slightly different title: "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem (extended abstract)," in *Crypto '82* [20], pp. 279-288.
- [102] —, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," *IEEE Trans. Informat. Theory*, vol. IT-30, no. 5, pp. 699-704, Sept. 1984.
- [103] Z. Shmueli, "Composite Diffie-Hellman public-key generating systems are hard to break," Computer Science Department, Technion, Haifa, Israel, Technical Rep. 356, Feb. 1985.
- [104] R. Silver, "The computation of indices modulo P ," Mitre Corporation, Working Paper WP-07062, p. 3, May 7, 1964.
- [105] G. J. Simmons and M. J. Norris, "Preliminary comments on the M.I.T. public key cryptosystem," *Cryptologia*, vol. 1, pp. 406-414, Oct. 1977.
- [106] G. J. Simmons, "Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques," in *IEEE EASCON '79* (Washington, DC), pp. 661-662, Oct. 9-11, 1979.
- [107] G. J. Simmons and M. J. Norris, "How to cipher faster using redundant number systems," Sandia National Laboratories, SAND-80-1886, Aug. 1980.
- [108] G. J. Simmons, "High speed arithmetic utilizing redundant number systems," in *National Telecommunications Conf.*, (Houston, TX), pp. 49.3.1-2, Nov. 30-Dec. 4, 1980.
- [109] —, Ed., *Secure Communications and Asymmetric Cryptosystems*. AAAS Selected Symposium 69. Boulder, CO: Westview Press, 1982.

- [130] —, "Cryptology," in *Encyclopaedia Britannica*, 16th Edition. Chicago, IL: Encyclopaedia Britannica, 1986, pp. 913-924B.
- [111] Proceedings of Smart Card 2000, Vienna, Austria, Oct. 19-20, 1988.
- [112] M. V. Wilkes, *Time-Sharing Computer Systems*. New York, NY: American Elsevier, 1972.
- [113] H. C. Williams, "A modification of the RSA public-key cryptosystem," *IEEE Trans. Informat. Theory*, vol. IT-26, no. 6, pp. 726-729, Nov. 1980.
- [114] —, Eds., *Advances in Cryptology-CRYPTO '85*. Berlin, Germany: Springer-Verlag, 1986.
- [115] S. Wolfram, "Cryptology with cellular automata," in *Crypto '85* [114], pp. 429-432.
- [116] M. C. Wunderlich, "Recent advances in the design and implementation of large integer factorization algorithms," in *1983 Symp. on Security and Privacy*, (Oakland, CA, pp. 67-74, Apr. 25-27, 1983).
- [117] K. Yau and K. Peterson, "A single-chip VLSI implementation of the discrete exponential public key distribution system," in *COMAC (Government Microcircuit Applications Conference)*, (Orlando, FL), pp. 18-23, Nov. 1982.



Whitfield Diffie was born in Washington, DC, on June 5, 1944. He received the B.S. degree in mathematics from the Massachusetts Institute of Technology, Cambridge, MA, in 1965.

While at Mitre Corporation from 1965 to 1969, he worked with Carl Engelman in developing the Mathlab symbolic mathematical manipulation system, later expanded at MIT to become Macsyma. In 1969, he transferred to the Stanford University Artificial Intelligence Laboratory to work with John McCarthy on proof checking and proof of correctness of programs. While there he also developed the compiler adopted for the U.C. Irvine Illisp system. In 1973, Diffie took leave from Stanford and began his work on cryptography while traveling around the U.S. He continued this work as a graduate student under Martin Hellman at Stanford University from 1975 through 1978. Since 1978, Diffie has been the Manager of Secure Systems Research for Bell-Northern Research, Mountain View, CA. His most recent work has been on key management protocols for telephones designed to operate on the developing Integrated Services Digital Network.

Exhibit W

Reg Art
time
1/17/79

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
MAR 2 1979

GROUP 220

In the matter of the application of :
Ronald Linn Rivest, Adi Shamir and :
Leonard Max Adleman :
Serial No: 860,586 : Examiner: H.A. Birmiel
Filed: December 14, 1977 : Group Art Unit: 222
For: CRYPTOGRAPHIC COMMUNICATIONS :
SYSTEM AND METHOD :

REQUEST FOR EXTENSION OF TIME

Hon. Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Dear Sir:

We request that the period for response to the Office Action of December 15, 1978 be extended for one month from March 15, 1979 to April 15, 1979. The Action set a three-month response period and the requested extension would be the first extension of that period.

The extension is requested to provide the applicants' attorney with further time to meet with the applicants to discuss the interview with the Examiner on this date, and to formulate an appropriate response in light of the issues discussed at that interview.

We enclose a copy of this Request and ask that the action taken on this Request be communicated to us on the copy.

Respectfully submitted,

KENWAY & DENNEY

By [Signature]
Mark G. Lappin
Reg. No. 261618

MGL:mrr

60 State Street
Boston, Massachusetts 02109
Tel: (617)227-6300
March 2, 1979

AUTHORITY OF THE PRIMARY EXAMINER
PERIOD FOR RESPONSE TO PAPER
MAILED Dec 12, 1978
IS EXTENDED TO RUN

MONTH(S) _____ WEEK(S) _____
DATE March 2, 1979

5/30/79
M



80.00 - 102-60-286

9
B + atts
L. Washington
5/31/79

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the matter of the application of :
: Ronald L. Rivest, Adi Shamir and :
: Leonard M. Adleman :
: Serial No: 860,586 ✓ :
: Filed: December 14, 1977 :
: For: CRYPTOGRAPHIC COMMUNICATIONS :
: SYSTEM AND METHOD :

Examiner: H.A. Birmiel
Group Art Unit: 222

RECEIVED
MAY 23 1979
GROUP 220

AMENDMENT A

Hon. Commissioner of Patents
Washington, D.C. 20231

Dear Sir:

This paper is responsive to the Office Action of
December 15, 1978. Please amend the above-referenced application
as follows:

IN THE CLAIMS:

Add the following claims:

Sub
C3
improper multiple class
filed before 01-24-78
B1

34. A system according to claims 1 or 2 or 3 or 4 or 5 or 6 or 7
or 8 or 9 or 10 or 11 or 12 or 13 or 14 or 15 or 16 or 17 or 28
or 29 or 30 wherein at least one of said transforming means
comprises:

a first register means for receiving and storing a
first digital signal representative of said word-to-be-
transformed,

a second register means for receiving and storing a
second digital signal representative of the exponent of the
equivalence relation defining said transformation,

a third register means for receiving and storing a
third digital signal representative of the modulus of the
equivalency relation defining said transformation, and

-1-

05/22/79 860586 3 102 80.00CK
59341 05/30/79 360586 11-0575 1 504 76.00CR

76

OK 76.00

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

- A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,
- B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,
- C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and
- D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

B' control

40
38, A method according to claims ²³ 18 or ²⁴ 19 or ²⁵ 20 or ²⁶ 21 or ²⁷ 22 or
28 ²⁹ 23 or ³⁰ 24 or ³¹ 25 or ³² 26 or ³³ 27 or ³⁴ 28 or ³⁵ 29 or ³⁶ 30 or ³⁷ 31 wherein at least one
of said transforming means comprises the steps of:

receiving and storing a first digital signal in a first register, said first digital signal being representative of said word-to-be-transformed,

receiving and storing a second digital signal in a second register, said second digital signal being representative of the exponent of the equivalence relation defining said transformation,

receiving and storing a third digital signal in a third register, said third digital signal being representative of the modulus of the equivalency relation defining said transformation, and

exponentiating said first digital signal by repeated squaring and multiplication using said second and third digital signals, said exponentiating step including the substeps of:

- A. receiving and storing a first multiplier signal in an output register, and applying said first multiplier signal to a first multiplier input line,
- B. successively selecting each of the bits of said second digital signal as a multiplier selector, and
- C. for each of said multiplier selectors, selecting as a second multiplier signal either the contents of said output register or the contents of said first register, and for applying said second multiplier signal to a second multiplier output line, said selection being dependent on the binary value of the successive bits of said second digital signal,
- D. for each of said multiplier selectors, generating

B'
cont'd

B'
concl'd

said first multiplier signal in a modulo multiplier in response to the first and second multiplier signals on said first and second multiplier input lines, and for transferring said generated first multiplier signal to said output register, said first multiplier signal initially being representative of binary 1 and thereafter being representative of the modulo product of said first and second multipliers, where the modulus of said modulo product corresponds to said third digital signal.

REMARKS:

The applicants' attorney gratefully acknowledges the Examiner's efforts extended at the interview of March 2, 1979.

Initially, it is noted that new claims 34 and 35 have been added. These claims are directed to cover applicants' invention in the form shown in Fig. 3. As agreed to by the Examiner at the interview, Fig. 3 clearly has sufficient hardware to support allowable claims. Accordingly, it is submitted that claims 34 and 35 are at least allowable combined with the claims from which they depend.

In the Office Action, all of claims 1-33 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Issue is taken with that position.

In the rejection, the Examiner states that "the present invention as claimed lies in a particular algorithm which is employed to implement the public key cryptography scheme of Diffie and Hellman (reference R). However, there are no mathematical algorithms in the applicants' claims.

The expressions in the applicants' claims which include

the symbol " \equiv " denote the well-known equivalence relation: congruence modulo m , for integers. The symbol " \equiv " merely is a shorthand notation (invented by Gauss in 1801) for expressing this equivalence relation to relate sets of numbers shown on either side of that symbol, in effect establishing a set of conditions between the related integers, or signals representative thereof. In Van Norstrand's Scientific Encyclopedia (Van Norstrand Reinhold Company, 1976, page 64), this equivalence relation is defined as follows:

Two elements a, b of a ring are congruent modulo m , written $a \equiv b \pmod{m}$, if there exist elements p, q, r in the ring such that $a = mp+r, b = mq+r$

Also see Stewart, B.M., Theory of Numbers, MacMillan Company, New York, 1952, pages 111, 112 (copy enclosed). Thus, the symbol " \equiv " is a symbol for "congruence", not arithmetic or mathematical "equality", and the fact that the equivalence relation of the form

$$A \equiv BC \pmod{n}$$

is in the claims does not introduce a mathematical formula or algorithm to the claims but rather describes a relationship between two signals, e.g. the message and ciphertext. More particularly, in the applicants' claims, the message M and the ciphertext C are related by the transformation performed by the encoding means and the ciphertext C is related to the receive message word M' by the transformation performed by the decoding means. The claims include a description of these relationships, but do not specify any algorithms for effecting the transformations.

It should be noted that there may be many algorithms

which may be used to obtain the various terms for the relation. For example, the "exponentiation by repeated squaring and multiplication" approach shown by applicants' in the preferred embodiment is but one way of finding terms satisfying the relation. However, applicants do not claim any particular algorithms. In fact, any algorithms which may be used in practicing applicants' invention may readily be used in other applications without being covered by the applicants' claims.

Thus, the applicants' claimed invention does not "lie in an algorithm" which is employed to implement the Diffie and Hellman scheme, as characterized by the Examiner, but rather resides in a step of or means for transforming an input signal to an output signal in a communications system so that the output signal is related to the input signal by the specified equivalency relation, regardless of the particular technique or algorithm employed in performing that transformation.

Moreover, it appears that the §101 rejection would not have even come into play in this case if the expressions of the equivalency relation were not present. This may be seen if it is assumed for the moment that the encoding and decoding (i.e. transforming) means of claim 1 were simple transformation means, for example, digital complimenting or inverter circuits. Then, the claim could have the form:

A cryptographic communications system comprising:

- A. a communications channel
- B. an encoding means coupled to said channel including means for digitally inverting a transmit message word M to form a ciphertext word C and for transmitting C on said channel
- C. a decoding means coupled to said channel and adapted for receiving C from said

channel and for inverting C to form a receive message word M'

This hypothetically claimed system has three basic elements: a communication channel and two inverters coupled thereto. The inverters perform a "mathematical transformation" on the signal applied to them. There is no algorithm specified for performing the inversion, but only a requirement that the ciphertext be related to the message by the complementing relation.

Assuming that digital complementing was a suitable transformation for the invention, and that the claimed structure satisfied 102 and 103, then there would be no question that the claims would be allowable. Section 101 would quite properly not come into play since there are merely three interconnected hardware elements. In the present case, the encoding and decoding means are merely somewhat more complex building blocks than inverter circuits, where each block performs a transformation on input signals applied to the block. As in the hypothetical claim, there is no particular formula or algorithm specified for the transformation in the applicants' claims--only that the resultant signal be related to the input signal by the stated equivalency relation.

The applicants merely use such a building block. While at the present time there may not be any single chip implementations of that building block available, the block may be readily built by those skilled in the art, for example by merely implementing the circuit shown in Fig. 3. The applicants by their claims certainly do not preempt the transformation performed by the building block. For these reasons, the Examiner's position that the claimed invention "lies in a particular algorithm" is incorrect. Accordingly, the rejection should be

reconsidered and withdrawn.

It is also noted that the rejection was applied against claims 1-17 and 28-30 which are system claims, as well as claims 18-27 and 31-33 which are method claims.

Regarding the method claims 18-27 and 31-33, the Examiner stated that the "invention as claimed lies in a particular algorithm . . .", citing Parker v. Flook, 198 U.S.P.Q. 193 and Gottschalk v. Benson, 175 U.S.P.Q. 673. The Examiner appears to use the term "algorithm" synonymously with the term "mathematical formula" found, for example, in the Benson case. The present invention, as claimed, does not fall within the proscribed subject matter of the Benson case, because it does not seek to patent a mathematical formula, and hence does not seek to patent an "algorithm" within the definition of mathematical formula set forth by Benson and Flook. As noted above, the claims 18-27 and 31-33 do not claim mathematical formulae but merely include expressions of an equivalence relation to pose conditions (expressed in Gauss' shorthand notation) on the claimed transformations.

The Court in Flook noted that "the only novel feature of the method is a mathematical formula", 198 U.S.P.Q. at 195. The Court goes on to state in footnote 1 on page 195 that "we use the word "algorithm" in this case as we did in Gottschalk v. Benson, . . ., to mean "a procedure for solving a given type of mathematical problem...". The subject matter claimed in the present case is neither a procedure for solving a mathematical problem, nor a hitherto unknown mathematical formula or a sequence of such mathematical formulae, but is instead the application of one or more process steps to establish cryptographic communications and to provide authentication of digital messages.

While some of these steps may be, and in fact are, expressed in part with an equivalence relation (i.e. using Gauss' shorthand notation), that fact does not implicate that those steps are claims to a mathematical formula or algorithm. In the present case, the applicants' claimed steps do not claim a mathematical formula or algorithm. This may be better seen if, for example, lines 13 and 14 of claim 18 were changed from "whereby $C \equiv M^e \pmod{n}$ " to an equivalent form which reads "by selecting C so that the difference between C and the eth power of M is an integer multiple of n." Clearly, there is no "algorithm" in this form of the claim. It does not matter how C is selected. For example, C may be selected by "trial-and-error", or alternatively by "exponentiation-by-repeated-squaring" (as in the applicants' preferred embodiment) or some other method. The exponentiation-by-repeated-squaring approach is of course considerably more efficient in terms of hardware implementation. But it is important to note that the claims are independent of any particular method (or algorithm) for finding the terms to satisfy the relation. All that matters is that these terms be found -- by any method or algorithm. This same reasoning is applicable to all of claims 1-33. Thus, the claimed invention is not a proscribed "algorithm" within 35 U.S.C. 101.

The CCPA cases which have evolved in the face of Benson and Flook (and which have not been reversed), cases such as In re Chatfield, 191 USPQ 730 (CCPA 1976), In re Freeman, 197 USPQ 464 (CCPA 1978), and In re Johnson, et al., 200 USPQ 199 (CCPA 1978), clearly support the proposition that the invention claimed herein is patentable under 35 U.S.C. 101. The Johnson decision (which was handed down after the Office Action herein) is particularly informative since it follows (in time and substance) the Flook

decision. In Johnson, the CCPA states:

"[I]t is clear after Flook that the board's conclusion that patent protection is proscribed for all inventions algorithmic in character is overbroad and erroneous."
(200 USPQ at 205)

The CCPA in Johnson further went on to solidify the definition of an algorithm, citing Chatfield, wherein they stated:

"The Supreme Court carefully supplied a definition of the particular algorithm before it, i.e., [a] procedure for solving a given type of mathematical problem.

"The broader definition of algorithm is a step-by-step procedure for solving a problem or accomplishing some end.... It is axiomatic that inventive minds seek and develop solutions to problems and step-by-step solutions often attain the status of patentable invention. It would be unnecessarily detrimental to our patent system to deny inventors patent protection on the sole ground that their contribution could be broadly termed an 'algorithm'."
(200 USPQ at 206-207)

The CCPA then went on to review the two step analytical approach taken in Freeman to determine whether or not the claims before it were patentable. The Court of Customs and Patent Appeals in Freeman dealt with method claims similar in form to the method claims rejected in the present case. The CCPA's analysis in that decision is directly applicable here. In Freeman, the Court set forth a two-step analysis for determination of whether a claim is directed to non-statutory subject matter as a whole, in light of Benson:

"First, it must be determined whether the claim directly or

indirectly recites an 'algorithm'
in the Benson sense of that term,....

"Second, the claim must be further
analyzed to ascertain whether in
its entirety it wholly preempts that
algorithm." (197 USPQ at 471)

In Freeman, the Court noted that every process may be characterized as a "step-by-step procedure...for accomplishing some end" and that therefore, it would be "absurd" to interpret the Supreme Court's view as encompassing all such processes. Even if that "absurd" interpretation were taken, in the present case, as discussed above, the rejected claims are not "algorithmic", in spite of the fact that the claims include an equivalence relation. That equivalence relation only expresses conditions on a transformation. The conditions expressed by that equivalence relation may not be characterized as "a step-by-step procedure...for accomplishing some end". Thus, the present rejection should be reconsidered and withdrawn for the same reasons cited in Freeman.

Even assuming that according to the first step of Freeman analysis, the process steps herein "directly or indirectly recite process steps which are themselves calculations, formulae, or equations" (which in applicants' opinion they do not), it is clear that the applicants' claims in no way wholly preempt any such calculations, formulae or equations. This may be seen, for example, by the fact that a congruency equivalence relation is found in the cipher system disclosed by the Stewart reference (copy enclosed with the applicants' prior art statement), but Stewart's approach is clearly not within the scope of the applicants' claims. Thus, the second step of the Freeman analysis leads to the inevitable conclusion that the claims herein clearly fall squarely within the Johnson analysis

and the present claims should be allowed.

Furthermore, following the remainder of Johnson reasoning, the CCPA elaborates upon its two part Freeman analysis to determine whether the claims recite mathematical algorithms which are non-statutory. Under the continuing second step analysis of the CCPA's reasoning, one

"must determine whether each claim as a whole, including all of its steps, merely recites a mathematical formula or a method of calculation. This analysis requires careful interpretation of each claim in the light of its supporting disclosure to determine whether or not it merely defines a method of solving a mathematical problem. If it does not, then it defines statutory subject matter, namely, a 'process'".
(200 USPQ 208, 209)

The invention in claims 18-27 and 31-33 is not directed to the solution of a mathematical problem, but rather solves the problem of privately transmitting a message over a communications channel and the problem of authentication (i.e. by providing digital signatures) of messages. The claims include the step of transforming a first signal to a second signal so that the second signal is related to the first by a stated equivalence relation. The method for doing so does not claim mathematical formulae and does not seek patents on a mathematical formula. Accordingly, the invention claimed herein clearly falls under the CCPA and Supreme Court reasonings.

For these reasons, the rejection of claims 18-27 and 31-33 under 35 U.S.C. 101 should be reconsidered and withdrawn.

With particular regard to system claims 1-17, and 28-30, it is noted that the Benson and Flook cases cited by the Examiner addressed method claims only. The Supreme Court in

Benson stated "The question is whether the method described and claimed is a 'process' within the meaning of the Patent Act." 175 USPQ at 674 (emphasis added). Similarly, in Flook, the Supreme Court addressed the question of whether a novel formula "makes an otherwise conventional method eligible for patent protection" 198 USPQ at 196. Thus, in both of the cited cases, the Supreme Court addressed "processes" under 35 U.S.C. 101.

In contrast, the claims 1-17 and 28-30 are all directed to apparatus including means to perform specified functions. Moreover, the claims are clearly supported in the specification by a hardware implementation of the claimed subject matter. Accordingly, the rejection of system claims 1-17 and 28-30 is inappropriate and should be reconsidered and withdrawn.


Moreover, even if the Examiner treats these system claims in the same manner as the method claims 18-27 and 31-33, the rejection should be withdrawn for the reasons discussed above in particular reference to the method claims.

For these reasons, the rejection of claims 1-33 under 35 U.S.C. 101 is inappropriate and should be withdrawn. It is submitted that these claims, as well as new claims 34 and 35 are in condition for allowance and passage to issue is requested.

Respectfully submitted,

KENWAY & JENNEY

By


Mark G. Lappin
Reg. No. 26,618

60 State Street
Boston, MA 02109
Tel: (617)227-6300
May 15, 1979

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D. C. 20231.

on MAY 15 1979
(Date of Deposit)

MARK G. LAPPIN

Name of applicant, assignee, or Registered Representative


Signature

MAY 15 1979
Date of Signature

Exhibit X

1 Jon Michaelson, Esq., (State Bar No. 083815)
2 Kurt H. Taylor, Esq., (State Bar No. 127077)
3 Robert W. Ricketson, Esq., (State Bar No. 148481)
4 HOPKINS & CARLEY
5 A Law Corporation
6 150 Almaden Boulevard, Fifteenth Floor
7 San Jose, California 95113-2089
8 Telephone: (408) 286-9800

9 Attorneys for Plaintiff
10 CYLINK CORPORATION

11 IN THE UNITED STATES DISTRICT COURT
12 IN AND FOR THE NORTHERN DISTRICT OF CALIFORNIA

13 CYLINK CORPORATION,
14 Plaintiff,

15 v.

16 RSA DATA SECURITY, INC.,
17 Defendants.

18 **CR 94 02332** No. **W**

19 **COMPLAINT FOR DECLARATORY
20 JUDGMENT AND INJUNCTIVE
21 RELIEF AND DEMAND FOR JURY
22 TRIAL**

23 1. Plaintiff Cylink Corporation is incorporated under the laws of the State of
24 California, and has its principal place of business therein.

25 2. Defendant RSA Data Security, Inc. ("RSADSI") is a corporation incorporated
26 under the laws of the State of Delaware, and has its principal and a regular and established place of
27 business at 100 Marine Boulevard, Redwood City, CA 94065.

28 3. Jurisdiction of this Court arises under the Federal Declaratory Judgments Act,
Title 28, United States Code, Sections 2201 and 2202, and under the laws of the United States
concerning actions relating to patents, Title 28, United States Code, Section 1338(a), as shown by the
facts alleged below.

4. On September 20, 1983, U.S. Letter Patent No. 4,405,829 entitled "Cryptographic
Communications System and Method" was issued to inventors and assignors R. Rivest, A. Shamir
and L. Adleman ("the Patent").

COMPLAINT FOR DECLARATORY
JUDGMENT AND INJUNCTIVE RELIEF

ORIGINAL

CMP

C
me
10/28/94
@ 1:30 PM

94 JUN 30 PM 4:13
FILED
N/P
U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
San Jose, California

1 5. Cylink is informed and believes and on that basis alleges that in or about 1984
2 defendant RSADSI obtained an exclusive license to the Patent.

3 6. Cylink has made and/or offered for sale within the past six years and since the
4 issuance of the said Letters Patent, certain encryption products.

5 7. Beginning in or about December 1993, RSADSI has charged that Cylink's
6 manufacture and sale of said encryption products infringes the Patent and all claims thereof. On June
7 28, 1993, RSADSI delivered to Cylink's wholly-owned subsidiary, in this judicial district, a letter
8 expressly stating RSADSI's intent to bring an infringement action against Cylink. A true and correct
9 copy of RSADSI's letter to Cylink dated June 29, 1994 is attached hereto as Exhibit A.

10 8. There is a substantial and continuing justiciable controversy between Cylink and
11 RSADSI as to RSADSI's right to threaten or maintain suit for infringement of the Patent, and as to the
12 validity, scope, and enforceability thereof, and as to whether any of Cylink's products infringes any
13 valid claim thereof.

14 9. Cylink is informed and believes and on that basis alleges that the Patent is invalid,
15 unenforceable, and void, for one or more of the following reasons:

16 (a) The alleged invention was not novel;

17 (b) The differences (if any) between the alleged invention and the prior art
18 were such that the alleged invention would have been obvious at the time made to a person having
19 ordinary skill in the art;

20 (c) The claims of the Patent, and/or the Patent as a whole, fails to meet one or
21 more of the requirements of 35 U.S.C. section 112.

22 (d) If there is any invention in the subject matter of the Patent, which is
23 denied, the Patent nevertheless was not obtained in a manner consistent with the provisions of
24 Title 35 of the United States Code.

25 (e) The claims of the Patent are functional, indefinite, and are broader than the
26 alleged invention as set forth in the specification of the Patent.

27 10. Cylink will seek leave of court to amend this complaint to assert such additional
28 grounds for invalidity as may be ascertained and shall give such notice prior to trial as may be

1 required by 35 U.S.C. section 282 of the matters specified therein.

2 11. Cylink is informed and believes and on that basis alleges that its encryption
3 products do not infringe on the Patent or its claims.

4 12. Cylink is informed and believes and on that basis alleges that the Patent is
5 unenforceable for reasons including, but not necessarily limited to the following:

6 (a) RSADSI, with full knowledge of the activities of Cylink, has failed to
7 assert the Patent for a period of 3 years while Cylink invested time and money in building its business
8 and goodwill, and RSADSI is now guilty of laches and cannot maintain any cause of action against
9 plaintiff under the Patent.

10 (b) Pursuant to certain written agreements, RSADSI has obligated itself to
11 license Cylink to make, use, and sell products employing all inventions claimed in the patent, and is
12 therefore estopped from asserting the Patent against Cylink. True and correct copies of these
13 agreements are attached hereto and incorporated in this complaint as Exhibits B and C.

14 13. RSADSI has denied that it is obligated to license Cylink as alleged in
15 paragraph 12(b) above. Cylink and its wholly owned subsidiary have initiated an arbitration
16 proceeding against RSADSI pursuant to the written agreements between the parties. By bringing this
17 suit, as it has been forced to do in order to protect itself against the threat of litigation by RSADSI,
18 Cylink does not waive its right to a determination through contractually mandated arbitration that
19 RSADSI is obligated to grant to Cylink a license to the Patent according to the terms of the parties'
20 agreements.

21 WHEREFORE, plaintiff demands:

22 (a) Entry of judgment that RSADSI is without right or authority to threaten or to
23 maintain suit against plaintiff or its customers for alleged infringement of Letters Patent No.
24 4,405,829; that the Patent is invalid, unenforceable, and void in law; and that the Patent is not
25 infringed by Cylink because of the making, selling, or using of any products made, sold, or used by
26 Cylink.

27 (b) Entry of a preliminary injunction enjoining RSADSI, its officers, agents, servants,
28 employees, and attorneys, and those persons in active concert or participation with it who receive

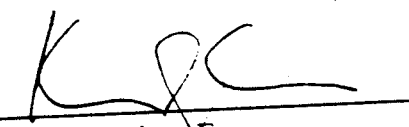
1 actual notice thereof from initiating infringement litigation and from threatening Cylink or any of its
2 customers, dealers, agents, servants, or employees, or any prospective or present seller, dealer, or user
3 of Cylink's products, with infringement litigation or charging any of them either verbally or in writing
4 with infringement of Letters Patent No. 4,405,829 because of the manufacture, use, sale, or offering
5 for sale of products made by Cylink, to be made permanent following trial.

6 (c) Entry of judgment for its costs and reasonable attorney fees incurred by Cylink
7 herein.

8 (d) Such other and further relief as the Court may deem appropriate.

9
10 DATED: June 30, 1994

HOPKINS & CARLEY
A Law Corporation

11
12 By: 
13 Kurt H. Taylor, Esq.
14 Attorneys for Plaintiff
15 CYLINK CORPORATION

16
17 **DEMAND FOR JURY TRIAL**

18 Cylink hereby demands trial by jury of all issues triable of right by jury.

19
20 DATED: June 30, 1994

HOPKINS & CARLEY
A Law Corporation

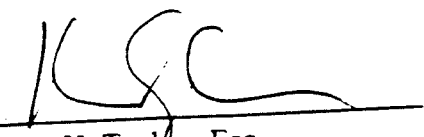
21
22 By: 
23 Kurt H. Taylor, Esq.
24 Attorneys for Plaintiff
25 CYLINK CORPORATION

Exhibit Y

Exhibit Z

On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them back.

SINK CLIPPER!



Because some things

What you can do...

BOYCOTT CLIPPER DEVICES AND

THE COMPANIES IN WHICH MAKE

THEM EXCLUSIVELY. Don't buy any-

thing with a Clipper Chip in it. Don't

buy any product with Big Brother in-

side when, beware of digital signature

systems that require the use of a

Capstone (Clipper) chip. It is likely that

the government will ask you to use Clip-

per for communications with the IRS,

or when doing business with federal

agencies. They cannot, as yet, require

you to do so. Remember, like people

spend YOUR money and work for

YOU, vote the shareholder cast a

vote now!

WRITE YOUR REPRESENTATIVES IN

WASHINGTON: Since there is nothing

quite as powerful as a letter from a con-

stituent, tell your own senators & repre-

sentative in Washington what you think

about the Clipper Proposal and the cur-

rent restrictions placed upon the export

of products which contain robust encryp-

tion technology. Tell them that you're

seriously concerned about the Clipper

Proposal's implications for the personal

privacy of U.S. citizens and the global

competitiveness of U.S. industry. They

may just care much about your privacy

in Washington, but they still care about

your vote.

ASK FOR RSA BY NAME: Be wary of soft-

ware and hardware product claims of

"security" or "encryption" ... many sys-

tems contain little more than home-

grown scrambling schemes, written by

developers with no background in cryp-

tography. Most of them are trivial to

break. Find out exactly what kind of

security you are getting in your next

e-mail, e-forms, cellular devices, operat-

ing system or remote access software pur-

chase. Whenever you shop for software

that makes claims about security, be sure

to ask the sales rep about which algo-

rithms are used inside. Demand the very

best in encryption: insist on RSA.

SUPPORT VENDORS THAT STILL PROP-

UCTS USING REAL RSA ENCRYPTION

TECHNOLOGY: Secured software and

hardware products that use RSA are avail-

able from: Alcatel TTN, ANS, CO-RE,

Apple, Bankers Trust Company, BDC

Development, Cinchmat, Mitrowave,

Cycomm, Cylink, Dalantech, Delrina,

Digital, Enterprise Solutions, Fictive In-

ternational, GE Information Services,

General Magic, Global Village, Hewlett-

Packard, Higrave, Hughes Aircraft,

IBM, Lotus, McCaw Cellular, Mitrosul,

Motorola, National Semiconducter,

Newbridge Networks, Nortel Telecom,

Novell, Oracle, PCSI, Rascal Datacom,

Because some things
are better left unread.



Red, Secure Communications Inc, Soma-
phone, Shana, Storage Tek, Sunsoft,
Trusted Information Systems, Unibus,
WordPerfect and many others. These
companies need to be acknowledged for
having the vision and courage to add ru-
bust cryptography to their products when
the US government has made it as pain-
ful as possible. Let them know you ap-
prove, and encourage others!

LEARN MORE: RSA Data Security main-
tains an extensive library of educational
materials on all aspects of the techni-
ques. RSA Laboratories' Frequent Asked
Questions About Today's Cryptography
is a great place to start, and it's free.

United States District Court

DISTRICT OF _____

Roger Schlafly

SUMMONS IN A CIVIL ACTION

v.

CASE NUMBER:

Public Key Partners, and
RSA Data Security Inc.

C⁻ -94 20512

TO: (Name and Address of Defendant)

Bob Fougner
Public Key Partners
310 N Mary Ave
Sunnyvale CA 94086

SW

PVT

YOU ARE HEREBY SUMMONED and required to file with the Clerk of this Court and serve upon

PLAINTIFF'S ATTORNEY (name and address)

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

an answer to the complaint which is herewith served upon you, within _____ days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.

RICHARD W. WIEKING

CLERK

JUL 27 1994

DATE

BERNADETTE FLORES-VIERA

BY DEPUTY CLERK

RETURN OF SERVICE

Service of the Summons and Complaint was made by me ¹	DATE
NAME OF SERVER (PRINT)	TITLE

Check one box below to indicate appropriate method of service

- Served personally upon the defendant. Place where served: _____

- Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
Name of person with whom the summons and complaint were left: _____
- Returned unexecuted: _____

- Other (specify): _____

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____
Date
Signature of Server

Address of Server

¹) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.

United States District Court

DISTRICT OF _____

Roger Schlafly

SUMMONS IN A CIVIL ACTION

v.

CASE NUMBER:

Public Key Partners, and
RSA Data Security Inc.

C - 94 20512

SW

TO: (Name and Address of Defendant)

Jim Bidzos, President
RSA Data Security
100 Marine Parkway
Redwood City, CA 94086
(415) 595-8782

PVT

YOU ARE HEREBY SUMMONED and required to file with the Clerk of this Court and serve upon

PLAINTIFF'S ATTORNEY (name and address)

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

an answer to the complaint which is herewith served upon you, within _____ days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.

CLERK RICHARD W. WIEKING
BERNADETTE FLORES-VIERA

JUL 27 1994
DATE _____

BY DEPUTY CLERK _____

RETURN OF SERVICE

Service of the Summons and Complaint was made by me ¹	DATE
NAME OF SERVER (PRINT)	TITLE

Check one box below to indicate appropriate method of service

- Served personally upon the defendant. Place where served: _____

- Left copies thereof at the defendant's dwelling house or usual place of abode with a person of suitable age and discretion then residing therein.
Name of person with whom the summons and complaint were left: _____
- Returned unexecuted: _____

- Other (specify): _____

STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on _____
Date
Signature of Server

Address of Server

¹) As to who may serve a summons see Rule 4 of the Federal Rules of Civil Procedure.