

## Quiz 1

1. This quiz is intended to provide a fair measure of your understanding of the course material to date (Homeworks 1–6 and Lectures 1–14).
2. Do not open this quiz booklet until the quiz begins. Read all the instructions first.
3. When the quiz begins, write your name on every page of this quiz booklet.
4. This quiz booklet contains ?? pages, including this one. An extra sheet of scratch paper is attached. If necessary, you can use it for the continuation of any problem answer.
5. This quiz is open-book, open-notes. No calculators or programmable devices (including laptop computers) are permitted.
6. Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Do not put part of the answer to one problem on the back of the sheet for another problem; pages may be separated for grading.
7. Partial credit will be given. You will be graded not only on the correctness of your answer, but also on the clarity with which you express it. Be neat.
8. Good luck!

Problem	Points	Grade	Initials
1	24		
2	42		
3	35		
4	18		
5	20		
6	20		
Total	159		

Your Name: \_\_\_\_\_

**Problem Q1-1. Short Answer** [24 points]

- (a) Professor Nibble's laptop was stolen last Monday. Apparently the good professor left his laptop on his desk and then went to get some coffee, neglecting to close his door in the process. The thief entered the building, took the elevator to the third floor, walked into the professor's office, removed the laptop from the desk, and then left the building. The theft illustrates that at least two security principles were not honored. Name one of them.

**Solution:** Failure to maintain a security perimeter; failure to provide for physical security.

- (b) Why do so many website privacy policies state that the websites are not for use by children under the age of 12?

**Solution:** Because the Children's Online Privacy Protect Act requires parental consent for children under 12. It's easier to officially prohibit children under 12 from using the website than to get consent.

- (c) Why does Amazon.com's website specifically state that its website may not be used by people under the age of 18?

**Solution:** Because people under 18 can't agree to binding legal contracts without the consent of their parents.

(d) How does Amazon.com enforce its policy?

**Solution:** It doesn't. The policy exists so that people can't refuse to pay for books under the grounds that the book was purchased by a child.

(e) The year is 2030. Due to advances in both nanotechnology and artificial intelligence, Moore's law has accelerated: starting in 2005, computers have been doubling in performance every year. Is the AES-128 standard still secure against well-funded nation-state attackers? How about AES-192 or AES-256? Explain your reasoning.

**Solution:** Given the assumptions of the problem, there will be roughly 25 doublings between today 2030. Thus, a 128-bit key in 2030 would have the same security as a 103-bit key today. Today most security professionals believe that an 80-bit key is secure (although just barely so). So even if computers double in performance every year, a 128-bit key should still be secure in the year 2030.

Of course, many people actually believe that Moore's Law is going to be slowing down, not accelerating...

(f) Ben Bitdiddle is designing the web interface for a local bank that will allow depositors to find their current balance from any web browser. To authenticate depositors Ben wants the depositors to use their social security number and a password that they are assigned when the account was created. Give two strengths and two weaknesses of this system.

**Solution:** Strengths: the bank can give users strong passwords. The system does not require additional hardware. Weaknesses: users may not be able to remember their passwords. Passwords may be grabbed by a keyboard logger.

**Problem Q1-2. True or False** [42 points]

Circle **True** or **False** for each of the following statements. If the statement consists of two parts where one part is true and the other part is false, circle False. No justification is required, but if you think the question is ambiguous, state your clarifying assumptions.

**True**   **False**     It takes between 50,000 times and 100,000 times the computing power to crack an 80-bit symmetric key as to crack a 64-bit key.

**Solution:** True.

**True**   **False**     Despite advances in number theory and factoring, 512-bit RSA keys remain secure for most applications because no 512-bit RSA key has ever been factored.

**Solution:** False.

**True**   **False**     In order to trust a Certificate Authority's X.509v3 Public Key, you need to sign it.

**Solution:** False. Placing a certificate containing the CA's public key in your "trusted certificate store" causes your computer to trust it.

**True**   **False**     An X.509 certificate that has expired can never be trusted.

**Solution:** False. You decide which certificates you trust and which certificates you do not trust.

**True**   **False**   There are more than 50 certificates containing CA private keys installed with Microsoft Internet Explorer

**Solution:** True. Amazing, isn't it?

**True**   **False**   In high security applications it is necessary to verify an entire public key, rather than simply the fingerprint of a public key, because different public keys occasionally have the same fingerprint.

**Solution:** False. Many other aspects of crypto systems fail if our hash functions start colliding. Since we are so utterly dependent upon them elsewhere, verifying a hash of a key is generally considered to be sufficient.

**True**   **False**   MD5 is generally believed to be weaker than SHA-1 because extremely small input files (less than 8 characters) occasionally have the same MD5 hash.

**Solution:** False. No two files have ever been found that have the same MD5 hash.

**True**   **False**   SHA-1 is more secure than MD5 because SHA-1 implements a Feistel Network.

**Solution:** False. SHA-1 does not implement a Feistel Network.

- True False** A password file consisting of usernames and Unix password hashes should be protected because the Unix password hash function can be inverted with a large expenditure of computer time.  
**Solution:** False. The password file needs to be protected because an attacker could do a dictionary attack — for any given password in the password file the attacker could read the salt, hash that salt with every word in the dictionary, and then see if the resulting hash is the password hash.
- True False** The CCIS Solaris systems (such as `denail.ccs.neu.edu`) require difficult-to-type and difficult-to-remember passwords because the encrypted password database is world-readable, and thus subject to a dictionary attack.  
**Solution:** True.
- True False** The original Unix password algorithm is believed to be collision-free for any input that can be easily typed.  
**Solution:** False. “Northeast” and “Northeastern” have the same hash, and they are both easily typed.
- True False** One theoretical way to find MD5 collisions is to identify loops in the space of all possible MD5 hashes. Once you have a map of the loops, you can find an MD5 collision by “riding the loop” — that is, by starting with the MD5 of the string you have and hashing until you find the MD5 of the string that you want.  
**Solution:** False. This will find a hash loop, but it won’t find you a collision.

- True False** Riding the loops isn't practical with today's computers, but the approach described in the previous question would work in theory if you had a computer that was fast enough and had enough memory.  
**Solution:** False, for the same reason as the previous question.
- True False** Given an infinite amount of computer time, it should be possible to take any 128-bit MD5 hash residue and derive the original input file.  
**Solution:** False. Because MD5 reduces the number of bits in the input to produce an output, there are many different inputs that map to a single output. An unbounded adversary (e.g., an "infinite" amount of computer time) could generate a list of possible inputs less than a given size that produce a single MD5, but it could not determine which input was responsible for that MD5.
- True False** It is not generally possible to recover overwritten information from modern hard drives using equipment that is commonly available at any of Boston's larger research universities.  
**Solution:** True.
- True False** Even if some of the blocks making up a Microsoft Word are overwritten on a computer's hard drive, it may still be possible to recover confidential information from the remaining blocks.  
**Solution:** True.

**True False** The tools that are used to analyze hard disk images work equally well with images of floppy disks, USB drives, CDRs, DVD-RAM, and most other forms of computer media.

**Solution:** True.

**True False** One practical way to stop spam would be to embark on a massive public education campaign that would convince people not to open unsolicited email and not to purchase products that are advertised in this fashion.

**Solution:** False.

**True False** One good way for a criminal to discover a user's password is to call up the user in question and ask, "what is your password?"

**Solution:** True.

**True False** When conducting a background investigation it is important to trade off the value of the information sought with the cost of obtaining the information.

**Solution:** True.

**True**   **False**   A one-time pad offers information theoretic perfect security, even from an unbounded adversary with infinite computing resources.

**Solution:** True.

**True**   **False**   One reason that it is important to force users to change their passwords on a regular basis is that occasionally two or more users are unknowingly sharing the same account.

**Solution:** True.

**True**   **False**   One reason that smart cards are gaining in popularity is that the cards contain high-speed processors that can perform cryptographic operations much faster than most desktop and laptop computers today.

**Solution:** False.

**True**   **False**   Today's fingerprint readers cannot be fooled by artificial means, but fingerprint readers should nevertheless not be trusted because the back-end database can be corrupted.

**Solution:** False: although the back-end database can be corrupted, fingerprint readers can be fooled by artificial means.

**Problem Q1-3. Multiple Choice** [35 points]

(a) How many strings  $s$  are there such that  $\text{SHA-1}(\text{MD5}(s)) = \text{MD5}(\text{SHA-1}(s))$

- (A) None
- (B) Precisely One
- (C) Precisely Two:  $\text{SHA-1}(s)$  and  $\text{MD5}(s)$ .
- (D) The actual number is unknown
- (E) The actual number is unknown, but at least one

*Solution Note:* SHA-1 is a 160-bit message digest while MD5 is a 128-bit digest, thus the values of the two functions can never be equal.

(b) A Certificate Authority's public key is trusted because:

- (A) The CA's public key is used to sign the CA's private key.
- (B) The CA's private key is used to sign the CA's public key.
- (C) The CA paid a lot of money to Microsoft or Netscape to put the CA's certificate into desktop operating system and/or web browsers.
- (D) The cryptographic hash of the public key appears in a secure store; this hash is verified when the certificate is downloaded by the web browser.
- (E) None of the above.

(c) Apples HCI guidelines on passwords recommend:

- (A) That programs accepting passwords require users to type the passwords twice, each time in a separate box. The computer should then verify that the two boxes are equal.
- (B) That the individual characters in a password be echoed when the password is typed, and then turned to dots when the cursor leaves the input box.
- (C) That the user interface support copy-and-paste so that a password displayed as dots can be copied into another program "without any loss of fidelity."
- (D) That double-clicking on the text in a password field should select all of the characters in the password.

(d) In their study of Kazaa usability, Good and Krekelberg found:

- (A) That the majority of Kazaa users are sharing information without their knowledge.
- (B) That files containing valid credit card numbers could be downloaded from other Kazaa users on the Internet.

- C That Kazaa's user interface is specifically designed to cause people to share information without their knowledge.
- D That installing Kazaa installs many programs that could be classified as spyware.
- E That some users do not understand that sharing a folder actually shares all of the files inside that folder, and not just the music files.
- F None of the above.

*Solution Note:* Answer A is probably true, but Good and Krekelberg did not conduct a survey of Kazaa's user base. Answer B isn't true because the authors did not download *other people's* spreadsheets containing credit-card numbers and try them out. Answer C is incorrect: while Good and Krekelberg found that the Kazaa user interface did cause some of their test subjects to share information without their knowledge, the authors couldn't have known if Kazaa was *specifically designed* for this purpose. Likewise, answer D is wrong: although Kazaa does install spyware/adware, this was not a finding of the usability study.

(e) In *Why Johnny Cant Encrypt*, Tygar and Whitten found that:

- A PGP's interface was confusing even by industry standards of the time, indicating that security developers generally do not have good training in GUI design.
- B PGP's documentation didn't agree with the program, causing confusion in the minds of people who read it.
- C Some users didn't know if they were sending email messages that were signed, sealed, or not.
- D One of the reasons that PGP 5.0 for the Macintosh was hard for people to use was that the program required a Eudora toolbar to be installed first.
- E None of the above.

(f) The Soft Tempest Fonts described by Kuhn and Anderson:

- A Have been incorporated into Apples anti-aliased screen fonts.
- B Are in Microsoft's Clear Type anti-alias system for LCD displays.
- C Were development as part of a research project designed to assist in a new copy protection system.
- D Are designed for use on color displays and probably wouldn't work on black-and-white systems.

**E** All of the above.

**F** None of the above.

- (g) Recall that Loughry and Umphress's paper *Information leakage in Optical Systems* define three classes of emitters:

Class 1	An emitter from which the device's operational state can be determined
Class 2	An emitter that gives an indication that data is being transmitted, but from which the actual data cannot be determined.
Class 3	An emitter from which the actual content of the communications can be determined.

Circle all of the following statements that are true:

- A** A flashing activity light on a USB drive is an example of a Class 3 emitter — that is, an emitter from which the information content of the message can be determined.
- B** The flashing Receive Data light on some modems can be either a Class 2 emitter or a Class 3 emitter, depending on the modem's internal circuitry.
- C** House lights dimming when an air conditioner turns on is an example of a Class 1 emitter as defined in the paper.
- D** The paper disproved the null hypothesis, that Class 3 emitters do not exist.
- E** Overall, the kind of information leakage described in the paper is of theoretical interest, since Class 3 emitters cannot be usefully observed at more than 10 feet.

**Problem Q1-4. Privacy Policies** [18 points]

In the summer of 2000 the Federal Trade Commission and several federal legislators proposed a series of policies or regulations that would help assure (or at least improve) online privacy. All of the proposals were based, in part, on the Code of Fair Information Practices that had been originally developed in the 1970s. But whereas the Code specified five basic principles, the FTC adopted a new, revised set of principles: *Notice*, *Choice*, *Access* and *Security*.

- (a) What group, agency, or governmental body formulated the original Code of Fair Information Practices?

**Solution:** The Code was based on a Commission sponsored by the Department of Health, Education and Welfare under the Nixon/Ford administrations.

- (b) What did the FTC mean by *Notice*? Give an example.

**Solution:** Notice means that companies need to give notice of the fact that they are collecting personal information, and explain what they are doing with this information. An example of notice is Amazon.com's posting of a privacy policy.

- (c) What do you think that FTC mean by *Choice*? Give an example.

**Solution:** Choice means that customers need to have a choice as to whether or not information will be collected. In practice, most customers are simply given the choice to use a website or not to use a website. An example of choice is Amazon.com making you consent to their terms-of-service as a precondition to using their service; if you choose not to give consent, they don't let you use the service.

(d) What did the FTC mean by *Access*? Give an example.

**Solution:** Access means that individuals should be given access to their personal information stored on a company's computer system. For example, Amazon allows you to see your record, including your name, address, and other information.

(e) What do you think that FTC mean by *Security*? Give an example.

**Solution:** Security means that the organization will employ technical measures to assure the protection of personal information. An example is Amazon's firewall.

(f) Each of the FTC's four principles loosely match one of the original Fair information Practices. One of the original practices was missing. What did that practice say? You can quote it exactly or you can summarize it.

**Solution:** The fifth FIP was that information collected for one purpose wouldn't be used for another purpose.

(g) Give an example of a modern business practice that violates the missing principle.

**Solution:** Selling a customer's name and address to a company that engages in targeted marketing.

**Problem Q1-5. PGP** [20 points]

PGP is a popular email encryption program. When you first use PGP, you must create a secret key and a public key. The private key is stored on the PGP “secret key ring” while the public key is stored on the PGP “public key ring.” To provide for additional security, the keys on the secret key ring are encrypted with a passphrase.

Each PGP secret key can have its own passphrase. The PGP program allows you to change a key’s passphrase.

- (a) Describe a way in which the pass phrase on the PGP secret key might be implemented.

**Solution:** the answer

Ben Bitdiddle has an internship working at the FBI's computer crime squad. His squad has captured a number of PGP-encrypted messages that were sent to Dudley Gothim, a suspected mobster. Dudley's house is under surveillance and his DSL line is being wiretapped. Every few weeks Dudley gets a series of PGP encrypted messages, after which he gets in his car, drives through a forest (losing his tail), and then returns several days later. Precisely one week after each of these incidents there are reports in the newspaper of a new set of valuable MP3 songs being released on the Kazaa peer-to-peer network.

Alyssa P. Hacker wants to know the contents of those email messages.

- (b) Give four different approaches by which the contents of the PGP-encrypted messages could be revealed.

**Solution:** There were many correct answers, including:

- Steal a copy of the secret key chain, then put a keystroke recorder on Dudley's computer and record his keystrokes.
- Use a hidden video camera to videotape him typing.
- Replace the copy of PGP with a program that emails out the unencrypted key ring after it is decrypted.
- Arrest Dudley and torture him until he reveals his PGP pass phrase.

**Problem Q1-6. HashPass** [20 points]

Ben has designed a new system for defeating spammers that he calls *Hash Pass*. Here is how it works. When any computer on the Internet opens an SMTP connection to Ben's computer on port 25 to send Ben a piece of email, Ben's computer responds with a challenge like this:

```
350 HashChallenge: [Word] [Value]
```

Where the [Word] is a space-delimited value (e.g. *Hello, Cheese, or 12345-5432-111*), and [Value] is a randomly-generated hexadecimal value such (e.g. *e, ef, ab3* or even *1234*). When faced with this challenge, the SMTP client must respond:

```
HashPass [Word+Suffix]
```

Where [WordSuffix]+ is a word where the MD5 of that word has the prefix of [Value] from above.

For example, if the client is presented with this challenge:

```
350 HashChallenge: SIMSON 5a54
```

A valid response would be:

```
HashPass SIMSON-EF
```

Because  $\text{MD5}(\text{"SIMSON-EF"}) = 5a5438731d1b15cb1de78f84fe69b86d$ .

Ben's idea is that Hash Passwords can be used as a kind of electronic postage for people sending email. When a known email client tries to send mail to Ben's server, no challenge needs to be issued. When a questionable server wants to send mail, a weak challenge can be sent. And when a mail server that appears to be a spammer wants to send an email message, Ben's computer can give a very hard challenge. This has the advantage over simply blocking email from the mail client that appears to be a spammer, because actual spammers won't accept the challenge — they will simply not send the email — whereas a legitimate sender will accept the challenge, take the time to solve the puzzle, and will be rewarded by having the email delivered.

- (a) Write a **HashChallenge** that is 65536 times harder than the **hashChallenge** presented in the problem description above.

**Solution:**

```
350 HashChallenge: SIMSON 5a540000
```

- (b) Give an efficient algorithm for solving the Hash Pass puzzle. You may describe the algorithm either with steps written in English, in pseudocode, or in any other unambiguous fashion.

**Solution:**

Ben's naive implementation of HashChallenges has a problem: sometimes the SMTP server presents challenges that cannot be solved in a reasonable amount of time. This became apparent on one day when Ben's server issued the HashChallenge:

```
350 HashChallenge deadbeef deadbeef
```

Is there a HashPass that will satisfy this HashChallenge? Why or why not?

(c) Ben takes his HashPass system to Alyssa and asks if his idea can be saved. “How can I modify my system so that the HashChallenges are always solvable?” he asks.

Alyssa rolls her eyes and shakes her head. “Ben,” she says, “you are approaching this problem in precisely the wrong way.”

Alyssa takes out a piece of paper and writes down an algorithm for creating HashChallenges that can always be solved.

Ben thanks Alyssa and goes back to his desk. Unfortunately, he loses the paper along the way. To save Ben the trouble of going back to Alyssa and facing her ridicule, please give Ben a workable algorithm below for generating HashChallenges

**Solution:**

(d) What would be required to have Ben's HashPass system deployed on the Internet today?

**Solution:**

SCRATCH PAPER