MATHEMATICAL GAMES

A new kind of cipher that would take millions of years to break

by Martin Gardner

"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

—EDGAR ALLAN POE

The upward creep of postal rates accompanied by the deterioration of postal service is a trend that may or may not continue, but as far as most private communication is concerned, in a few decades it probably will not matter. The reason is simple. The transfer of information will probably be much faster and much cheaper by "electronic mail" than by conventional postal systems. Before long it should be possible to go to any telephone, insert a message into an attachment and dial a number. The telephone at the other end will print out the message at once.

Government agencies and large businesses will presumably be the first to make extensive use of electronic mail, followed by small businesses and private individuals. When this starts to happen, it will become increasingly desirable to have fast, efficient ciphers to safeguard information from electronic eavesdroppers. A similar problem is involved in protecting private information stored in computer memory banks from snoopers who have access to the memory through data-processing networks.

It is hardly surprising that in recent years a number of mathematicians have asked themselves: Is it possible to devise a cipher that can be rapidly encoded and decoded by computer, can be used repeatedly without changing the key and is unbreakable by sophisticated cryptanalysis? The surprising answer is yes. The breakthrough is scarcely two years old, yet it bids fair to revolutionize the entire field of secret communications. Indeed, it is so revolutionary that all previous ciphers, together with the techniques for cracking them, may soon fade into oblivion.

An unbreakable code can be unbreakable in theory or unbreakable only in practice. Edgar Allan Poe, who fancied himself a skilled cryptanalyst, was convinced that no cipher could be invented that could not also be "unriddled." Poe was certainly wrong. Ciphers that are unbreakable even in theory have been in use for half a century. They are "one-time pads," ciphers that are used only once, for a single message. Here is a simple example based on a shift cipher, sometimes called a Caesar cipher because Julius Caesar used it.

First write the alphabet, followed by the digits 0 through 9. (For coding purposes 0 represents a space between words, and the other digits are assigned to punctuation marks.) Below this write the same sequence cyclically shifted to the right by an arbitrary number of units, as is shown in color in the illustration on this page. Our cipher consists in taking each symbol in the plaintext (the message), finding it in the top row, and replacing it with the symbol directly below it. The result is a simple substitution cipher, easily broken by any amateur.

In spite of its simplicity, a shift cipher can be the basis of a truly unbreakable code. The trick is simply to use a different shift cipher for each symbol in the plaintext, each time choosing the amount of shift at random. This is easily done with the spinner shown in the top illustration on the opposite page. Suppose the first word of plaintext is THE.

We spin the arrow and it stops on X. This tells us to use for encoding t a Caesar cipher in which the lower alphabet is shifted 10 steps to the right, bringing a below x as is shown in the illustration. t, therefore, is encoded as x. The same procedure is followed for every symbol in the plaintext. Before each symbol is encoded, the arrow is spun and the lower sequence is shifted accordingly. The result is a ciphertext starting with x and a cipher "key" starting with k. Note that the cipher key will be the same length as the plaintext.

To use this one-time cipher for sending a message to someone—call him Z—we must first send Z the key. This can be done by a trusted courier. Later we send to Z, perhaps by radio, the ciphertext, Z decodes it with the key and then destroys the key. The key must not be used again because if two such ciphers were intercepted, a cryptanalyst might have sufficient structure for breaking them.

It is easy to see why the one-time cipher is uncrackable even in principle. Since each symbol can be represented by any other symbol, and each choice of representation is completely random, there is no internal pattern. To put it another way, in order to achieve having the same length as the ciphertext is as legitimate as decoding an any as other. Even if the plaintext of such a coded message is found, it is of no future help to the cryptanalyst because the next time the system is used the randomly chosen key will be entirely different.

One-time pads are in constant use today for special messages between high military commanders, and between governments and their high-ranking agents. The "pad" is no more than a long list of random numbers, perhaps printed on many pages. The sender and receiver must of course have duplicate copies. The sender uses page 1 for a cipher, then destroys the page. The receiver uses his page 1 for decoding, then destroys his page. When the Russian agent Rudolf Abel was captured in New York in 1957, he had an one-time pad in the form of a booklet about the size of a postage stamp. David Kahn, who tells the story in his marvelous history The Codebreakers, says that the one-time pad is the standard method of secret radio communication used by the U.S.S.R. The famous "hot line" between Washington and Moscow also makes use of a one-time pad, the keys being periodically delivered through the two embassies.

If the one-time pad provides absolute secrecy, why is it not used for all secret communications? The answer is that it is too impractical. Each time it is employed a key must be sent in advance, and the key must be at least as long as the anticipated message. "The problem of producing, distributing, registering, and canceling the keys," writes Kahn, "may seem slight to an individual who has not had experience with military communications, but in wartime the volumes of traffic stagger even the signal staffs. Hundreds of thousands of words may be enciphered in a day; simply to generate the millions of key characters required would be enormously expensive and time-consuming. Since each

A Caesar cipher with a 10-shift
message must have its unique key, application of the ideal system would require shipping out on tape at the very least the equivalent of the total communications volume of a war.

Let us qualify Poe's dictum by applying it only to ciphers that are used repeatedly without any change in the key. Until recently all cipher systems of this kind were known to be theoretically breakable provided the code breaker has enough time and enough ciphertext. Then in 1975 a new kind of cipher was proposed that radically altered the situation by supplying a new definition of "unbreakable," a definition that comes from the branch of computer science known as complexity theory. These new ciphers are not absolutely unbreakable in the sense of the one-time pad, but in practice they are unbreakable in a much stronger sense than any cipher previously designed for widespread use. In principle these new ciphers can be broken, but only by computer programs that run for millions of years!

The two men responsible for this remarkable breakthrough are Whitfield Diffie and Martin E. Hellman, both electrical engineers at Stanford University. Their work was partly supported by the National Science Foundation in 1975 and was reported in their paper "New Directions in Cryptography" (IEEE Transactions on Information Theory, November, 1976). In it Diffie and Hellman show how to create unbreakable ciphers that do not require advance sending of a key or even concealment of the method of encoding. The ciphers can be efficiently encoded and decoded, they can be used over and over again and there is a bonus: the system also provides an "electronic signature" that, unlike a written signature, cannot be forged. If Z receives a "signed" message from A, the signature proves to Z that A actually sent the message. Moreover, A's signature cannot be forged by an eavesdropper or even by Z himself.

These seemingly impossible feats are made possible by what Diffie and Hellman call a trapdoor one-way function. Such a function has the following properties: (1) it will change any positive integer x to a unique positive integer y; (2) it has an inverse function that changes y back to x; (3) efficient algorithms exist for computing both the forward function and its inverse; (4) if only the function and its forward algorithm are known, it is computationally infeasible to discover the inverse algorithm. The last property is the curious one that gives the function its name. It is like a trapdoor: easy to drop through but hard to get up through. Indeed, it is impossible to get up through the door unless one knows where the secret button is hidden. The button symbolizes the "trapdoor information." Without it one cannot open the door from below, but the button is so carefully concealed that the probability of finding it is practically zero.

Before giving a specific example, let us see how such functions make the new cryptographic systems possible. Suppose there is a group of businessmen who want to communicate secrets to one another. Each devises his own trapdoor function with its forward and backward algorithms. A handbook is published in which each company's encoding (forward) algorithm is given in full. The decoding (inverse) algorithms are kept secret. The handbook is public. Anyone can consult it and use it for sending a secret message to any listed company.

Suppose you are not a member of the group but you want to send a secret message to member Z. First you change your plaintext to a long number, using a standard procedure given in the handbook. You then look up Z's forward algorithm and your computer uses it for rapid encoding of the ciphertext. This new number is sent to Z. It does not matter at all if the ciphertext is overheard or intercepted because only Z knows his secret decoding procedure. There is no way a curious cryptanalyst, studying Z's public encoding algorithm, can discover Z's decoding algorithm. In principle he might find it, but in practice that would require a supercomputer and a few million years of running time.

An outsider cannot "sign" a message to Z, but any member of the group can.

Here is the devilishly clever way the signature works. Suppose A wants to send a message to Z. He first encodes the plaintext number by using his own secret inverse algorithm. Then he encodes the ciphertext number a second time, using Z's public algorithm. After Z receives the ciphertext he first transforms it by applying his own secret decoding algorithm, then he applies A's public encoding algorithm. Out comes the message! Z knows that only A could have sent this doubly encoded ciphertext because it made use of A's secret algorithm. A's "signature" is clearly unforgeable. Z cannot use it to send a message purporting to come from A because Z still does.

A ciphertext challenge worth $100

<table>
<thead>
<tr>
<th>9666</th>
<th>9613</th>
<th>7546</th>
<th>2206</th>
</tr>
</thead>
<tbody>
<tr>
<td>1477</td>
<td>1409</td>
<td>2225</td>
<td>4355</td>
</tr>
<tr>
<td>6829</td>
<td>6575</td>
<td>9991</td>
<td>1245</td>
</tr>
<tr>
<td>7431</td>
<td>9674</td>
<td>6951</td>
<td>2093</td>
</tr>
<tr>
<td>0816</td>
<td>2682</td>
<td>2514</td>
<td>5708</td>
</tr>
<tr>
<td>3569</td>
<td>3147</td>
<td>9622</td>
<td>8839</td>
</tr>
<tr>
<td>8962</td>
<td>6013</td>
<td>3919</td>
<td>9055</td>
</tr>
<tr>
<td>1829</td>
<td>9451</td>
<td>5781</td>
<td>5154</td>
</tr>
</tbody>
</table>
The answers to last month's bisection problems:

1. The answer is the rectangle.

2. The answer is the square.

3. The answer is the triangle.

4. The answer is the parallelogram.

5. The answer is the rhombus.

6. The answer is the trapezoid.

7. The answer is the pentagon.

8. The answer is the hexagon.

9. The answer is the heptagon.

10. The answer is the octagon.

11. The answer is the nonagon.

12. The answer is the decagon.

Dividing polyominos into four congruent parts:

- The solution is shown in the diagram.
quired computer time between the two kinds of testing. For example, to test a 139-digit odd number for primality requires at the most (that is, when the number actually is prime) about seven minutes on a PDP-10 computer. The same algorithm takes only 45 seconds to find the first prime after 2350. (It is a 61-digit number equal to $2^{200} + 235$.)

Contrast this with the difficulty of finding the two prime factors of a 125- or 126-digit number obtained by multiplying two 63-digit primes. If the best algorithm known and the fastest of today's computers were used, Rivest estimates that the running time required would be about 40 quadrillion years! (For a good discussion of computer methods of factoring into primes, see Donald E. Knuth's *Seminumerical Algorithms*, Section 4.5.4.) It is this practical impossibility, in any foreseeable future, of factoring the product of two large primes that makes the M.I.T. public-key cipher system possible.

To explain how the system works, the M.I.T. authors take as an example of plaintext a paraphrase of a remark in Shakespeare's *Julius Caesar* (Act 1, Scene 2): *IT'S ALL GREEK TO ME.*

This is first changed to a single number, using the standard key: $a = 01, b = 02, \ldots, z = 26$, with 0 indicating a space between words. The number is 09201090011212000718050511002015001035.

The entire number is now encoded by raising it to a fixed power $s$, modulo a certain composite number $r$. The composite $r$ is obtained by randomly selecting (using a procedure given in the M.I.T. memorandum) two primes, $p$ and $q$, each of which is at least 40 digits long, and multiplying them together. The number $s$ must be relatively prime to $p-1$ and $q-1$. Numbers $r$ and $s$ are made public, to be used in the encoding algorithm. The encoding operation can be done very efficiently even for enormous values of $r$; indeed, it requires less than a second of computer time.

The two prime factors of $r$ are withheld, to play a role in the secret inverse algorithm. This inverse algorithm, used for decoding, consists in raising the ciphertext number to another power $i$, then reducing it to modulo $r$. As before, this takes less than a second of computer time. The number $i$, however, can be calculated only by someone who knows $p$ and $q$, the two primes that are kept secret.

If the message is too long to be handled as a single number, it can be broken up into two or more blocks and each block can be treated as a separate number. I shall not go into more details. They are a bit technical but are clearly explained in the M.I.T. memorandum.

To encode a message of any length, the M.I.T. group has chosen $s = 9,007$ and $r = 1143512570778877469235779976146801201289267212423625625618429357069352457338978305791235639587035058989075147599290026879543541$.

The number $r$ is the product of a 64-digit prime $p$ and a 65-digit prime $q$, each randomly selected. The encoding algorithm changes the plaintext number (09201...) to the following ciphertext number: 199905130149780510045231712374026604742320401750831463103703174062597760894267504399029062732882765012893554461353823769748026.

As a challenge to *Scientific American* readers the M.I.T. group has encoded another message, using the same public algorithm. The ciphertext is shown in the bottom illustration on page 121. Its plaintext is an English sentence. It was first changed to a number by the standard key: $A = 01, B = 02, \ldots, Z = 26$, with 0 indicating a space between words. The number is 1092096267258267501289355446135301D32 J15 83 hi 21783 500'8446929j)626l55.

The signature was added by which it was produced. Even in the unlikely event that the M.I.T. system is breakable there are probably all kinds of other trapdoor functions that can provide virtually unbreakable ciphers. Diffie and Hellman are applying for patents on cipher devices based on trapdoor functions they have not yet disclosed. Computers and complexity theory are pushing cryptog-
A Cipher that Defeated Poe

"Ge Jeasgdxv,  
Zij gl mw, laam, zxy zmiwhfzex ejydvxx kwke tx lbv aqgh lbmx anau bai Vamukks rwn vtlk agh gnumk wdlzweg jnbyxx oaeq enwzb zmngy mo mwlnw bx b al psfcdpsh wzex lssf xkiyahlh. Mk num yexdm wbxv sbl hlv wyx Plhkwnmcruk?"

In 1839, in a regular column Edgar Allan Poe contributed to a Philadelphia periodical, *Alexander's Weekly Messenger*, Poe challenged readers to send him cryptograms (monoalphabetic substitution ciphers), asserting that he would solve them all "forthwith." One G. W. Kulp submitted a ciphertext in longhand.

It was printed as shown above in the issue of February 26, 1840. Poe "proved" in a subsequent column that the cipher was a hoax—"a jargon of random characters having no meaning whatsoever."

In 1973 Brian J. Winkel, a mathematician at Albion College, and Mark Lyster, a chemistry major in Winkel's cryptian at Albion College, and Mark Lyster each found a 18-sided polygonal tetrad with bilateral symmetry.

A backtrack program by Golomb and Taylor finally found a solution for order 7, which was the largest TAD of this type.

Solomon W. Golomb proposed three further candidates for further investigation:

1. If all numbers in a TAD of order greater than 5 are distinct but not consecutive, how big is the largest number forced to be? (Example: An order-6 TAD is possible with the largest number as low as 22.)

2. Using all numbers from 1 to k, but allowing repeats, how big can k be in a TAD of order n? (Example: An order-6 TAD is possible with k as high as 20.)

3. For what orders is it possible to form a TAD modulo m, where m is the number of elements in the triangle and the numbers are consecutive from 1 to m? Each difference is expressed modulo m. Such triangles can be rotated so that every element below the top row is the sum (modulo m) of the two numbers above it. Here, in rotated form, are the four order-4 solutions:

<table>
<thead>
<tr>
<th>1</th>
<th>6</th>
<th>9</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>

A backtack program by Golomb and Taylor found no solution for order 5. Col. George Sicherman, who invented the original pool-ball problem, reports a computer proof of impossibility for order 6. Higher orders remain open.

Robert Ammann, Greg Frederickson, and Jean L. Loyer each found an 18-sided polygonal tetrad with bilateral symmetry (see illustration on this page), thus improving on the 22-sided solution I had published.

Dan Eilers, Allen I. Janis, Scott Kim, P. H. Lyons, Robert Mathews (with Martin G. Wallser), James Newton and Mike Tempest each found a second solution earlier this year, and after the testing tour on the order-5 square.

When I ended the column with limericks of decreasing length, I referred to the one-line limerick as the "last of four." Draper L. Kaufman, John L. Thomas D. Nehrer and James C. Viber were the first of many who told me I should have called it the last-but-one of five. The fifth, of course, has no lines, which is why other readers failed to notice it.

Tom Wright of Ganges, British Columbia, wrote: "I was interested in the limerick paradox, particularly in the decreasing two-line and one-line limericks. I wondered if you had, in fact, added the one-line limerick (about the man from Nepal), and I looked minutely to see if it wasn't there. On examination, my first impulse was to assume that it was indeed not there, since no space was provided, but further cogitation suggested that a no-line poem, requiring no space, might indeed be there. Unable to resolve this paradox by any logical proof, I am abjectly reduced to asking you whether or not a no-line limerick was not printed in the space not provided, or not."

A bilaterally symmetric tetrad with 18 sides