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 communication. Indeed, it is so revolutionary that all previous ciphers, together with the techniques for cracking them, may soon fade into oblivion.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A Caesar cipher with a 10-shift

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 K. 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 K as is shown in the illustration. T, therefore, is encoded as J. 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 J 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 ciphertexts 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, any message whatever having the same length as the ciphertext is as legitimate a decoding as any 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 a 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 embassiés.

If the one-time pad provides absolute secrecy, why is it not used for all secret communication? 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, registering, distributing 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

messag
cation
shippi
equiva
volum
Let
ing it
peated
Until
kind
breaka
has en
Then i
propos
ation
"unbre
from
known
cipher
in the
practic
strong
ly desi
ciple t
but onl
for mil
The
marka
Diffie
electri
sity. T
by the
in 197
per "N
(*IEEE*
ory, N
Hellm
able ci
sendin
the m
can be
they c
and th
provid
unlike
forged
from
A actu
A's sig
eavesd
The
made
man c
Such a
erties:
teger *x*
it has a
back t
for co
tion an
tion a
known
to disc
The
that gi
a trap
hard t
possibl
less on
is hid
"trapd
cannot
the bu

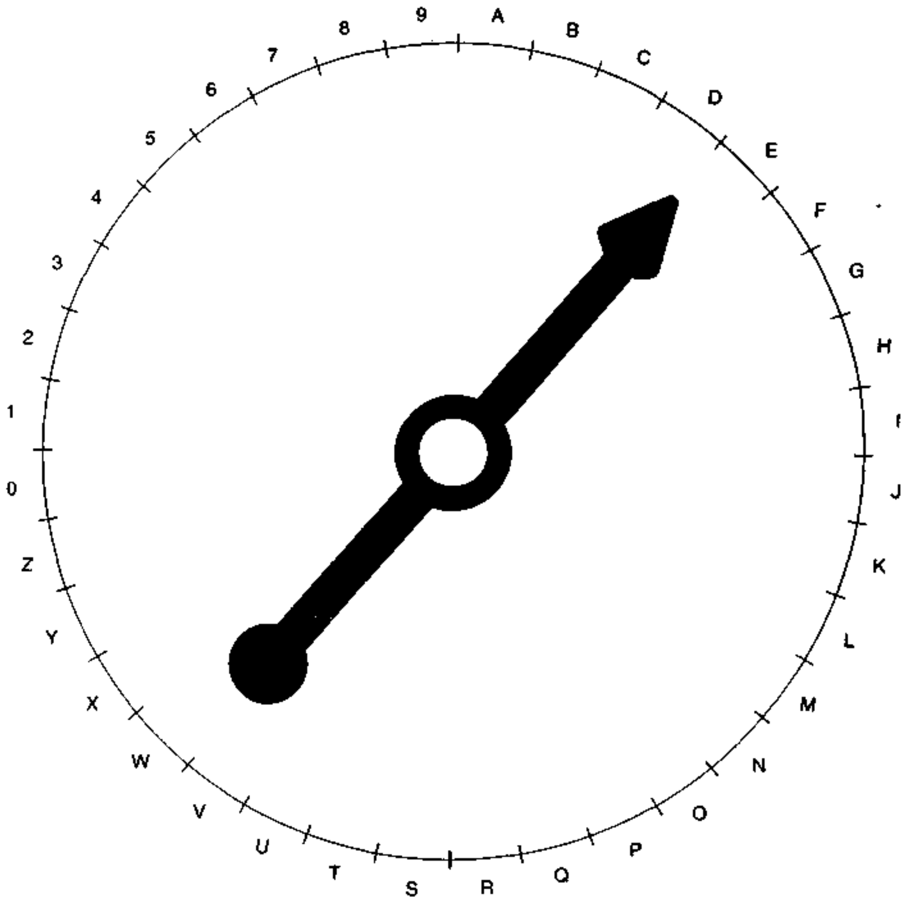
message must have its unique key, application of the ideal system would require shipping out on tape at the very least the equivalent of the total communications volume of a war."

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.



Randomizer for encoding a "one-time pad"

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.

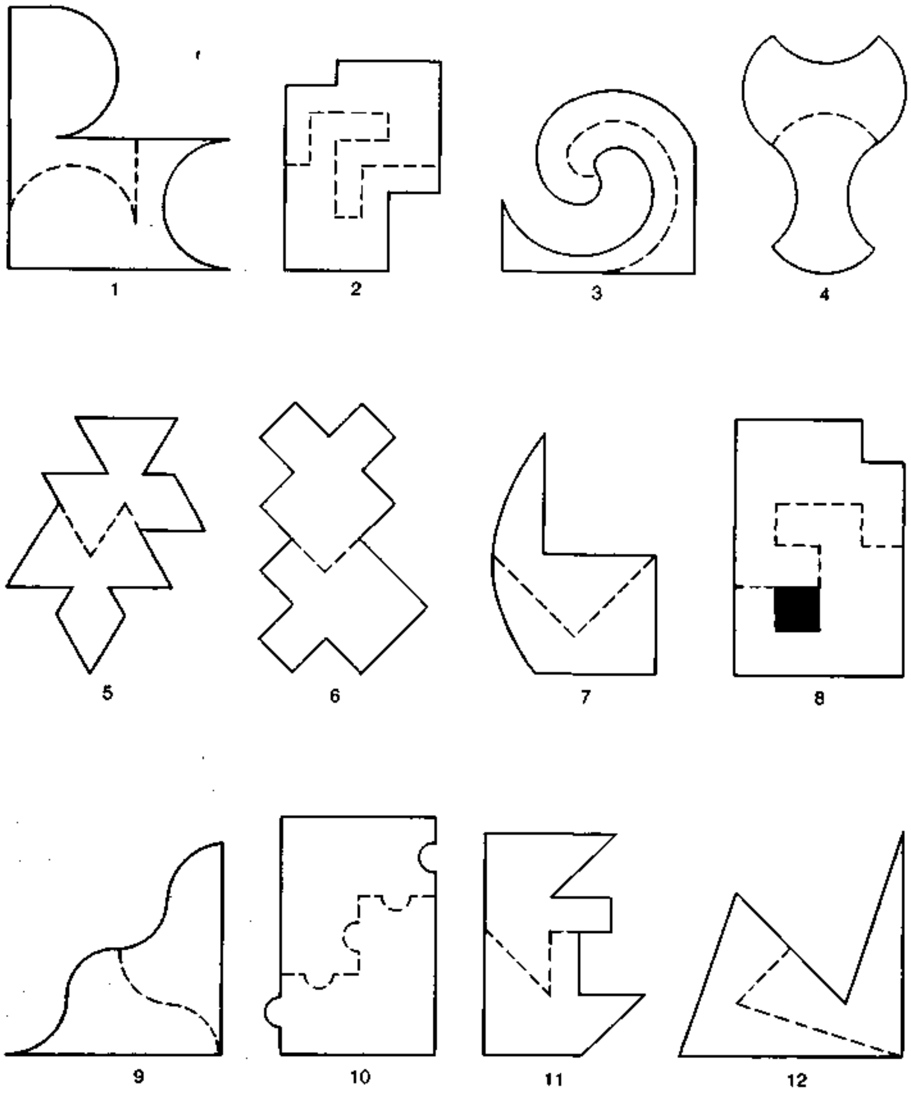
Suppose you are not a member of the group but you want to send a secret message to member *Z*. First you change your plaintext to a long number, using a standard procedure given in the handbook. Next you look up *Z*'s forward algorithm and your computer uses it for rapid encoding of the ciphertext. This 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 sign 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!

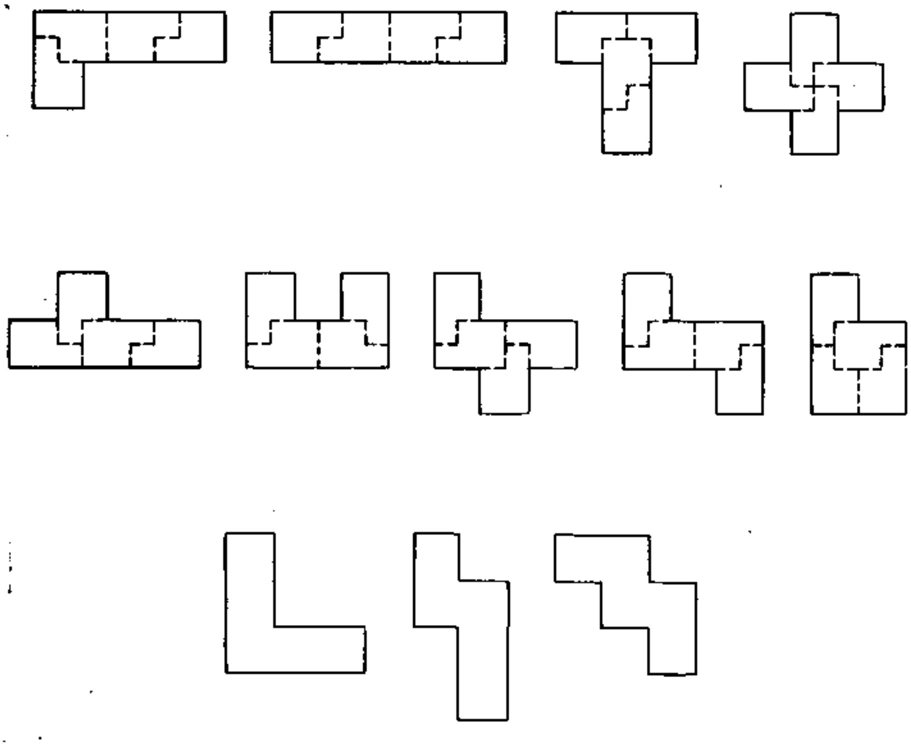
Z knows that only *A* could have sent this doubly encoded ciphertext because it made use of *A*'s secret algorithm. *A*'s "signature" is clearly unforgeable. *Z* cannot use it to send a message purporting to come from *A* because *Z* still does

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

A ciphertext challenge worth $100



The answers to last month's bisection problems



Dividing polyominoes into four congruent parts

not know *A*'s secret decoding algorithm. Not only that, but if it were to become necessary at some future time to prove to a third party, say a judge in a court of law, that *A* did in fact send the message, this can be done in a way that neither *A*, *Z* nor anyone else can dispute.

Diffie and Hellman suggested in their paper a variety of trapdoor functions that might be used for such systems. None is quite what is desired, but early this year there was a second breakthrough. Ronald L. Rivest, Adi Shamir and Leonard Adleman, computer scientists at the Massachusetts Institute of Technology, developed an elegant way to implement the Diffie-Hellman system by using prime numbers.

Rivest obtained his doctorate in computer science from Stanford University in 1973 and is now an associate professor at M.I.T. Once he had hit on the brilliant idea of using primes for a public cipher system, he and his two collaborators had little difficulty finding a simple way to do it. Their work, supported by grants from the NSF and the Office of Naval Research, appears in *On Digital Signatures and Public-Key Cryptosystems* (Technical Memo 82, April, 1977), issued by the Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, Mass. 02139. The memorandum is free to anyone who writes Rivest at the above address enclosing a self-addressed, 9-by-12-inch clasp envelope with 35 cents in postage.

To explain Rivest's system we need a bit of background in prime-number theory. The fastest-known computer programs for deciding whether a number is prime or composite (the product of primes) are based on a famous theory of Fermat's stating that if p is prime, and a is any positive number less than p, then $a^{p-1} = 1$ (modulo p). Suppose we want to test a large odd number n (all primes except 2 are of course odd) for primality. A number a is selected at random and raised to the power of $n - 1$, then divided by n. If the remainder is not 1, n cannot be prime. For example, $2^{21-1} = 4$ (modulo 21), therefore 21 is composite. What, however, is the connection between 2 (the randomly chosen a) and 3 and 7, the two prime factors of 21? There seems to be no connection whatever. For this reason Fermat's test is useless in finding prime factors. It does, however, provide a fast way of proving that a number is composite. Moreover, if an odd number passes the Fermat test with a certain number of random a's, it is almost certainly prime.

This is not the place to go into more details about computer algorithms for testing primality, which are extremely fast, or algorithms for factoring composites, all of which are infuriatingly slow. I content myself with the following facts, provided by Rivest. They dramatize the staggering gap in the re-

quired
kinds
130-di
quires
numbe
minute
same a
find th
digit n

Con
finding
or 126-
plying
algorit
day's c
mates
would
(For a
metho
Donald
rithms,
imposs
of fact
primes
cipher

To ex
M.I.T.
plainte
Shakes
Scene 2

This
ber, usi
= 02. . .
space b
092019
001305.

The e
raising
certain
posite r
ing (usi
M.I.T. r
q, each
and m
number
$p - 1$ a
made p
algorith
be done
mous va
than a s

The t
held, to
algorith
for dec
phertext
then red
this take
time. T
calculat
p and q.
secret.

If the
dled as a
up into
block ca
ber. I sl
They ar
explaine

To en
the M.I.
and r =
7997614

orithm.
become
o prove
:ourt of
ıessage.
ither *A*.

in their
ınctions
ystems.
ıt early
break-
Shamir
r scien-
tute of
ınt way
system

n com-
iversity
profes-
on the
a pub-
collab-
; a sim-
ıported
ıffice of
Digital
systems
77), is-
ɔmput-
tute of
ɜquare,
memo-
writes
closing
asp en-

need a
ıer the-
:r pro-
nber is
uct of
:ory of
, and *a*
ɒ, then
: want
ɔrimes
·imali-
ındom
, then
is not
ımple.
21 is
: con-
hosen
ors of
ɛction
's test
ɔrs. It
ay of
ıosite.
es the
ıer of
·rime.
more
ıs for
ɛmely
com-
ating-
e fol-
They
ıe re-

quired computer time between the two kinds of testing. For example, to test a 130-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 2^{200}. (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): ITS ALL GREEK TO ME.

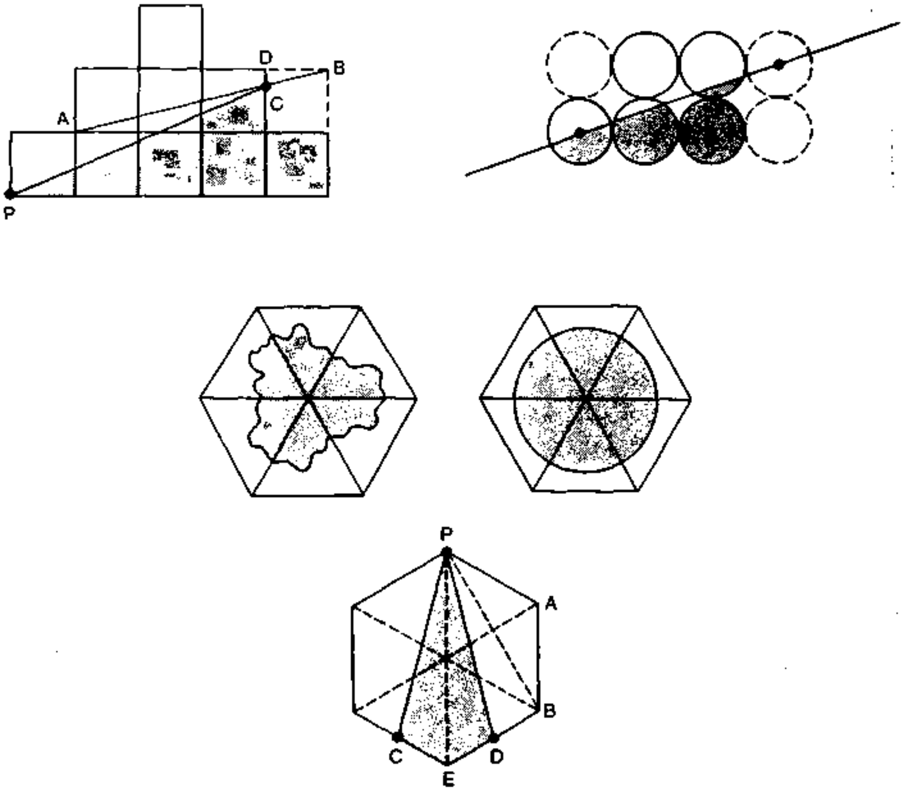
This is first changed to a single number, using the standard key: A = 01, B = 02, . . . , Z = 26, with 00 indicating a space between words. The number is 0920190001121200071805051100201 5001305.

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 *s* and *r* 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 *t*, then reducing it to modulo *r*. As before, this takes less than a second of computer time. The number *t*, 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. memo.

To encode ITS ALL GREEK TO ME, the M.I.T. group has chosen $s = 9{,}007$ and $r =$ 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.



Solutions to four equal-division problems

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: 1999351314978051004523171227402606474232040170583914631037037174062597160894892750430992096267258267501289355446135382376974802 6.

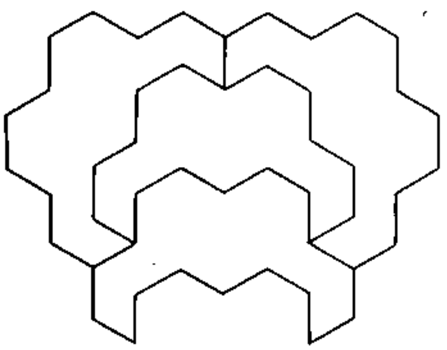
As a challenge to *Scientific American* readers the M.I.T. group has encoded another message, using the same public algorithm. The ciphertext is shown in the bottom illustration on page 121. Its plaintext is an English sentence. It was first changed to a number by the standard method explained above, then the entire number was raised to the 9,007th power (modulo *r*) by the shortcut method given in the memorandum. To the first person who decodes this message the M.I.T. group will give $100.

To prove that the offer actually comes from the M.I.T. group, the following signature has been added: 16717861150380844246015271389168398245436901032358311217835038446929062655448792237114490509578608655662496577974840004057020373.

The signature was encoded by using the secret inverse of the encoding algorithm. Since the reader has no public encoding algorithm of his own, the second encoding operation has been omitted. Any reader who has access to a computer and the instructions in the M.I.T. memorandum can easily read the signature by applying the M.I.T. group's public encoding algorithm, that is, by raising the above number to the power of 9,007, then reducing it to modulo *r*. The result is 06091819200019151222051800230914190015140500082114041805040004151212011819. It translates (by the use of the standard key) to FIRST SOLVER WINS ONE HUNDRED DOLLARS. This signed ciphertext could only come from the M.I.T. group because only its members know the inverse algorithm by which it was produced.

Rivest and his associates have no proof that at some future time no one will discover a fast algorithm for factoring composites as large as the *r* they used or will break their cipher by some other scheme they have not thought of. They consider both possibilities extremely remote. Of course any cipher system that cannot be proved unbreakable in the absolute sense of one-time pads is open to sophisticated attacks by modern cryptanalysts who are trained mathematicians with powerful computers at their elbow. If the M.I.T. cipher withstands such attacks, as it seems almost certain it will, Poe's dictum will be hard to defend in any form.

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 bilaterally symmetric tetrad with 18 sides

raphy into an exciting phase, and one that may be tinged with sadness. All over the world there are clever men and women, some of them geniuses, who have devoted their lives to the mastery of modern cryptanalysis. Since World War II even those government and military ciphers that are not one-time pads have become so difficult to break that the talents of these experts have gradually become less useful. Now these people are standing on trapdoors that are about to spring open and drop them completely from sight.

The top illustration on page 122 shows how the 12 shapes given last month can be divided into congruent halves. The bottom illustration on the same page shows how nine of the 12 order-5 polyominoes can be dissected into the same four congruent parts. The three blank polyominoes cannot be cut into four congruent parts of any shape.

The illustration on the preceding page answers the four problems at the end of last month's column. To bisect the nine squares draw the 10th square shown with broken lines. Rule *AB* to get point *C*, then join *P* to *C*. If the squares have sides of length 1, then *CD* equals 1/4, and it is easy to see that *PC* bisects the original figure. To bisect the five circles add three additional circles as shown by the broken lines. The line through the centers of two circles obviously halves the total area. (Both problems are from *A Problem a Day*, by R. M. Lucey, Penguin Books, 1937.)

The hexagon at the bottom is trisected by joining *P* to *C* and *D*, the midpoints of two sides. Assume that the equilateral triangles have areas of 1. The area of *PAB* is 1, therefore the area of *PBE* is 2 and the rest follows. I was unable to find any comparably simple way to trisect a regular pentagon with a line through a corner.

The middle two hexagons show how Leo Moser proved that the minimum-length curve bisecting an equilateral triangle is the arc of a circle. Whatever the shape of the bisecting curve, it will form a closed curve if the triangle is reflected around one vertex as is shown. Such a curve cuts the hexagon in half, and it has a fixed area. The figure of minimum perimeter that encloses a given area is the circle, therefore the minimum-length bisecting curves inside each triangle are arcs of a circle. (This exercise is from *Mathematical Quickies*, by Charles W. Trigg, McGraw-Hill, 1967.)

Comments on the mail response to April's short problems follow:

The generalization of the pool-ball problem to triangles of order *n*, bearing consecutive numbers starting with 1, has been solved. Herbert Taylor found an ingenious way to prove that no TAD (triangle of absolute differences) could be made with triangular arrays of order 9 or higher. Computer programs eliminated TAD's of orders 6, 7 and 8, therefore the unique solution for the 15 pool balls is the largest TAD of this type.

Solomon W. Golomb proposed three 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:

```
1 6 9 4   2 7 8 3   6 1 4 9   7 2 3 8
 7 5 3     9 5 1     7 5 3     9 5 1
  2 8       4 6       2 8       4 6
   0         0         0         0
```

A backtrack 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 (there are no more) for the lost-king 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. Kauffman, John Little, John McKay, Thomas D. Nehrer and James C. Vibber 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 no-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 Cipher that Defeated Poe

"Ge Jeasgdxv,

Zij gl mw, laam, xzy zmlwhfzek ejlvdxw kwke tx lbr atgh lbmx aanu bai Vsmukkss pwn vlwk agh gnumk wdlnzweg jnbxvv oaeg enwb zwmgy mo mlw wnbx mw al pnfdcfpkh wzkex hssf xkiyahul. Mk num yexdm wbxy sbc hv wyx Phwkgnamcuk?"

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 1975 Brian J. Winkel, a mathematician at Albion College, and Mark Lyster, a chemistry major in Winkel's cryptology class, cracked Kulp's cipher. It is not a simple substitution—Poe was right—but neither is it nonsense. Poe can hardly be blamed for his opinion. In addition to a major error by Kulp there are 15 minor errors, probably printer's mistakes in reading the longhand.

Winkel is an editor of a new quarterly, *Cryptologia*, available from Albion College, Albion, Mich. 49224, at $16 per year. The magazine stresses the mathematical and computational aspects of cryptology. The first issue (January, 1977) tells the story of Kulp's cipher and gives it as a challenge to readers. So far only three readers have broken it. I shall give the solution next month.