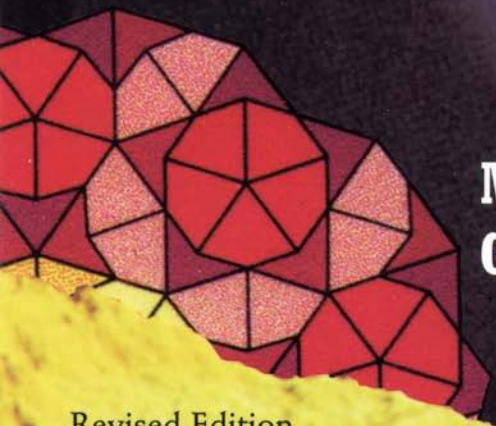
PENROSE TILES TO TRAPDOOR CIPHERS

...AND THE RETURN OF DR. MATRIX



Martin Gardner

Revised Edition

The Mathematical Association of America

CHAPTER 13

Trapdoor Ciphers

> 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 surely 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 infor-

mation 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,

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, MI 49224. 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 in the answer section.

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 Figure 90. 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 Figure 91. 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

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

Figure 90
A Caesar cipher with a 10-shift

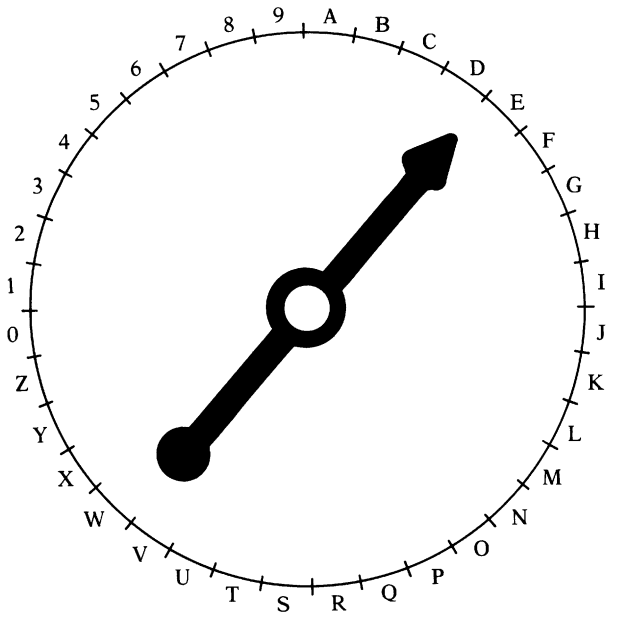


Figure 91 *Randomizer for encoding a "one-time pad"*

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 embassies.

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 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 three men responsible for this remarkable breakthrough are Whitfield Diffie and Martin E. Hellman, both electrical engineers at Stanford University, and Ralph Merkle, then an undergraduate at the University of California, Berkeley. Their work was partly supported by the National Science Foundation in 1975 and was reported by Diffie and Hellman in their 1976 paper "New Directions in Cryptography". 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. 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 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 in 1977 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 *A Method of Obtaining 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, MA 02139.

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 fac-

tors. 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 required 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 09201900011212000718050511002015001305.

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 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 $s = 9007$ and $r =$ 1143816257578888676692357799761466120102182967212423 6256256184293570693524573389783059712356395870505898907514759929002687954354 1.

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: 1999351314978051004523171227402606474232040170583914631037037174062597160894892750430992096267258267501289355446135382376974 8026.

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 Figure 92. 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 9007th 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: 1671786115038084424601527138916839824543690103235831121783503844692906265544879223711449050957860865566249657797484000405702037 3.

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

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

Figure 92
A ciphertext challenge worth $100

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 modulo r. The result is 0609181 92000191512220518002309141900151405000821140418050400041512 12011819. It translates (by the use of the standard key) to FIRST SOLVER WINS ONE HUNDRED DOLLARS. This signed ciphertext could come only 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 cryptography 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 possibly drop them completely from sight.

ANSWERS

In spite of the many errors in the published version of the cipher Poe could not solve, about a dozen readers, including 16-year-old James H. Andres, were able to crack it. The plaintext is as follows:

MR. ALEXANDER,
HOW IS IT, THAT, THE MESSENGER ARRIVES HERE AT THE SAME TIME WITH THE SATURDAY COURIER AND OTHER SATURDAY PAPERS WHEN ACCORDING TO THE DATE IT IS PUBLISHED THREE DAYS PREVIOUS. IS THE FAULT WITH YOU OR THE POSTMASTERS?

The cipher is a polyalphabetic substitution cipher working with 12 alphabets keyed by the words "United States." Each letter indicates the degree of shift for a Caesar cipher. Thus the alphabet key for M, the first letter of the plaintext, is A = U, B = V, C = W and so on. For R, the second letter of the plaintext, the key is A = N, B = O, C = P and so on.

There were 16 errors in the published cryptogram: first, J was given as the third letter instead of I, and second, the fifth letter in the message was omitted. If the second mistake had not been made, Poe might have guessed the opening to be "Mr. Alexander" and the solution would have followed easily.

As for the $100 challenge cipher, no one has cracked it. Rivest told me in 1988 that he no longer has a record of the message or the primes he used. However, since I gave the public key, he will be able to verify a solution if he receives one.

CHAPTER 14

Trapdoor Ciphers II

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

When I wrote the preceding chapter for a column in the August 1977 issue of *Scientific American*, I certainly had not anticipated the intense furor it would arouse. As I reported, Ronald Rivest had offered to send a copy of the M.I.T. memo giving details about what soon came to be known as the RSA cryptosystem (after the initials of the three mathematicians) to anyone who sent M.I.T. a stamped self-addressed envelope. This offer prompted Joseph Meyer, an angry employee of NSA (National Security Agency), to fire off threatening letters to the leaders of a coming symposium on cryptography, warning them that public disclosures of trapdoor systems violated national security laws.

M.I.T. had been flooded with some 7,000 requests from all over the world for its trapdoor-cipher memo, but Meyers's letter put a stop to the mailing. It was almost a year before M.I.T. attorneys concluded that the memo violated no laws and allowed the mailing to be resumed. Since then an uneasy truce has prevailed between NSA and researchers on public-key cryptosystems. There has been no outright censorship and no one has gone to jail, but there has been much voluntary censorship by mathematicians. High-level research within NSA remains top secret, and it is impossible for outsiders such as myself to know what NSA knows. The acronym NSA, it has often been said, stands for "Never Say Any-

thing" or (reflecting NSA's efforts to keep out of the limelight) "No Such Agency."

It is not hard to understand why NSA became so jittery. Publication of seemingly break-proof ciphers obviously allows other nations to adopt codes that NSA might be unable to crack, and, as long as there is freedom here to publish techniques for breaking such ciphers, any nation using a breakable code would at once stop using it. Moreover, as I implied, if truly unbreakable codes become common around the world, it would almost put NSA out of business.*

For many years U.S. banks and corporations have been protecting their communications with a system called Data-Encryption Standards (DES), developed by IBM and approved by the National Bureau of Standards. The DES is a "symmetric" system, meaning that it codes and decodes by the same procedure, not an "asymmetric" trapdoor system. Nevertheless, it is extremely difficult to break if its key uses a large number of bits. There is evidence that NSA persuaded IBM to hold its key size down to 56 bits so that in case foreign governments chose to adopt DES, NSA could still break their codes. Although DES is still being used, Bell Telephone rejected it for security reasons, and it has come under heavy fire, especially from Diffie and Hellman, who consider it too weak to survive many more years.

Chief rivals to the RSA system have been the so-called knapsack systems. Knapsack problems are a large family of combinatorial tasks that involve finding among a set of numbers a subset that will "fit," subject to various constraints, inside a hypothetical "knapsack." The simplest example, known as the subset-sum problem, is to select from a set of integers a subset that will add to a specified value. Subset-sum problems are common in the puzzle books of Sam Loyd and Henry Dudeney, often in the form of a target whose concentric rings are assigned different numerical values. The task is to determine how shots can be fired at the target to obtain hits that add exactly to a given sum. Such puzzles are not hard to solve by trial and error when the set of numbers is small, but they become enormously difficult as the set increases in size.

A combinatorial task is called "hard" if it can be shown that no computer algorithm can solve it in "polynomial time." This results from

*A good discussion of the pros and cons of the debate between NSA's desire for security and the mathematical community's desire for openness will be found in David Kahn's 1983 book, *Kahn on Codes*, pp. 198–203.

the fact that as a certain parameter of the problem increases, the time required to solve the problem grows at an exponential, or "nonpolynomial," rate. Studies of such problems belong to a new branch of mathematics and computer science called "complexity theory." A great deal of work has been done and is continuing on a special class of problems called NP-complete (NP for nondeterministic-polynomial). There are now hundreds of such problems, all believed to be hard (though no proof has yet been found), and all related so that if an algorithm is found for solving one of them in polynomial time, it will at once solve all of them. The subset-sum problem is NP-complete.

Ralph Merkle was the first to base a knapsack system on subset-sum, and for a short time it was preferred to RSA because it was faster to code and decode. Then in 1982 Adi Shamir, the Israeli member of the M.I.T. team, found an algorithm that solved "almost all" knapsack systems in polynomial time. Ralph Merkle had offered a $100 prize to anyone breaking his system, and Shamir collected it. Merkle then increased the complexity of his system to what he called a "multiply iterated" version, offering $1,000 to anyone who could break it. Ernest Brickell of Sandia Laboratories won the second prize in 1984. The subset-sum problem continues, however, to be NP-complete, and it is possible that new cipher systems based on it or on other knapsack problems will withstand the onslaught of new algorithms. Rivest and B. Chor have proposed a knapsack system based on the logarithms of large primes that has not so far been cracked by the Sandia techniques. It has been reported that NSA thought of knapsack codes about a decade before Merkle did but, in keeping with its "Never Say Anything" policy, has kept mum about it.

The factoring of large numbers is not in the NP-complete family, but it is thought to be hard, and so far no one has found a way to factor large numbers in polynomial time. However, such techniques have been steadily improving along with methods of testing the primality of big numbers. Fast procedures for testing primality in "near polynomial time" were discovered in the 1980's, and in 1982 a team at Sandia Labs, under the direction of Gustavus Simmons, succeeded (with a Cray supercomputer) in factoring the Mersenne number $2^{521} - 1$, an integer of 157 digits. It took the Cray about 32 hours to find the number's three prime factors. Until this breakthrough, mathematicians had estimated that a Cray computer would need millions of years to factor a number with more than 100 digits.

In view of these new factoring techniques, no one can rule out the possibility of a polynomial-time algorithm that would topple the RSA system. When the system was first announced, numbers of 80 digits were

recommended for the two primes p and q. It is now recommended that each of these primes be at least 100 digits. It is best that they be nearly the same size, that p plus or minus 1 and q plus or minus 1 should each have at least one large prime factor and that the greatest common divisor of $p - 1$ and $q - 1$ be fairly small. Up to now the RSA system has remained secure. Computer chips for fast coding and decoding are available from RSA Data Security, Inc., 10 Twin Dolphin Drive, Redwood City, CA 94065.

A variety of fascinating spin-offs have resulted from the basic ideas behind trapdoor codes. It occurred at once to Robert Floyd, a computer scientist at Stanford, that such systems could be used by two people in communication by mail (paper or electronic) to make random decisions in ways that are immune to cheating. For example, two people in touch by telephone can agree on the outcome of a random flip of a coin or the outcome of a die toss. In June 1978 Floyd sent me a letter outlining how two persons could play backgammon by mail or telephone. Picking up Floyd's cue, Rivest, Shamir and Adleman wrote a paper on "mental poker" in which they explained how two players who did not trust each other can actually play a fair game of poker over the phone without using any cards.*

Another spin-off was the development of ingenious systems for making secure the transmission of scientific data over electronic networks. Consider, for instance, research conducted by instruments that have been landed on Mars. Researchers need to be sure that when they link to these instruments, they are not linked to some other data source and that no one else can alter the data being transmitted or can alter their instructions to the instruments. In brief, they need to be assured of the network's authenticity, integrity and secrecy.†

The most startling, almost unbelievable, spin-off has been the development of what are called "zero-knowledge proofs." Suppose a mathematician discovers a proof of a certain theorem. He wants to convince his colleagues that he actually has the proof but doesn't want to disclose the proof itself. In 1986 it was shown that this could be done with special

*"Mental Poker" was first published in 1979 as a technical report of the M.I.T. Laboratory of Computer Science. It is reprinted in *The Mathematical Gardner*, edited by David Klarner (Prindle, Weber, and Schmidt, 1981). On coin flipping, see "Coin Flipping by Telephone," Manuel Blum, *SIGACT News*, 15, 1983, pp. 23–27.

†For a good summary of recent developments in this area of "telescience," see Peter Denning's "Security of Data in Networks," in *American Scientist*, 75, January/February 1987, pp. 12–14. For more detailed information see Dorothy Denning's book *Cryptography and Data Security* (Addison-Wesley, 1982).

cases of NP-complete problems. For example, consider the NP-complete task of finding a Hamiltonian circuit—a path that goes through all points of a graph just once and returns to the starting point. Suppose that for a given graph with a large number of points it is not known whether it has a Hamiltonian circuit. A mathematician wishes to convince his colleague that he has found such a circuit, but he doesn't want to reveal the actual circuit. It is hard to comprehend, but there are now techniques by which he can do this.

In 1986 Manuel Blum, a computer expert at the University of California, Berkeley, found a way to apply zero-knowledge proofs to *any* mathematical problem! The procedure consists essentially of a dialogue between the "prover" and the "verifier" who wants to be convinced that the proof exists. The verifier asks a series of random questions, each to be answered by yes or no. After the first question, the verifier is convinced that the prover has a 1/2 chance of being wrong. After the second question, he is convinced the prover has a 1/4 chance of being wrong. After the third question, the probability drops to 1/8, and so on, with the denominators increasing in a doubling series. After, say, 100 questions the chance that the prover is lying or doesn't have a proof becomes so close to zero that the verifier is convinced beyond any shadow of a doubt. After 300 questions the denominator is 2^{300}, which is more than the number of atoms in the universe. There is never absolute certainty that the proof exists, but it is so close to certainty that all doubt vanishes. See the Bibliography for some nontechnical pieces about this surprising new development.

Do zero-knowledge proofs have practical applications beyond satisfying the egos of mathematicians who want to announce a discovery before anyone else does and before they have published the details? They do indeed. Adi Shamir, now at the Weizman Institute in Israel, found a way to make use of zero-knowledge methods for creating unforgeable ID cards. Think of a computer chip within such a card that can engage in rapid dialogue with a computer chip in an instrument used for verifying the ID. Within a few seconds enough random questions have been asked and answered to convince the verifier "beyond any shadow of a doubt," even though the verification cannot be absolutely certain. There have for decades been methods of showing that large numbers are almost certainly prime, such as by using probabilistic techniques, but finding similar methods for validating an ID card came as a big surprise.

The implications of unforgeable ID cards for military as well as civilian use are so enormous that when Shamir applied for a U.S. patent, the Army ordered that all documents and materials related to such cards

be destroyed. This aroused such a storm of protest from the mathematical community that the government quickly rescinded the order, giving as its reason that it could not impose such restraints on a mathematician who was not a U.S. citizen. No one knows if NSA had any role in this attempt at censorship. For a good account of the flap, see the *New York Times* 1987 article cited in the Bibliography.

Inventions of new public-key cryptosystems and new ways to break them, as well as their applications to the security of networks and to identification techniques, are occurring so rapidly that by the time you read this chapter, much of it may be out of date. The science of cryptology is undergoing a curious revolution, and no one can predict just where it will lead. Let me close with some whimsical dialogue from *Romanoff and Juliet*, a play by Peter Ustinov first produced in New York City in 1957.

The scene occurs at the close of the second act. The General (played by Ustinov) is president of what is identified only as the smallest nation in Europe. Hooper Molesworth is the country's American ambassador. Vadim Romanoff is the Russian ambassador. Molesworth's daughter Juliet and Romanoff's son Igor are lovers.

In the American Embassy, the General says to Molesworth:

> "Incidentally, they [the Russians] know your code."
>
> Molesworth replies: "We know they know our code. We only give them things we want them to know."

Crossing over to the Russian Embassy, the General remarks to Romanoff:

> "Incidentally, they [the Americans] know you know their code."
>
> Romanoff says: "That does not surprise me in the least. We have known for some time that they knew we knew their code. We have acted accordingly—by pretending to be duped."

Returning to the American Embassy, the General says to Molesworth:

> "Incidentally, you know—they know you know they know you know. . . . "

Molesworth is now genuinely alarmed.

"What? Are you sure?"

"I'm positive."

"Thank you—thank you! I shan't forget this."

The General is amazed.

"You mean you didn't know?"

"No!"

In 1957 a dialogue like this was at least believable. Could it occur today? Maybe NSA knows.

BIBLIOGRAPHY

Books on cryptanalysis

Cryptanalysis. Helen Gaines. Dover, 1956. Reprint of a 1939 book.

The Codebreakers. David Kahn. Macmillan, 1967. Supersedes all previous histories.

Elementary Cryptanalysis. A. Sinkov. Random House, 1968.

Cryptography: A Primer. Alan Konheim. Wiley, 1981.

Codes, Ciphers, and Computers. Bruce Bosworth. Hayden, 1982.

Cryptography: A New Dimension in Computer Data Security. C. H. Meyer and S. M. Matyas. Wiley, 1982.

Kahn on Codes: New Secrets of Cryptology. David Kahn. Macmillan, 1983.

Codes, Ciphers, and Secret Writing. Martin Gardner. Dover, 1984. Reprint of a 1972 book for children.

Cryptographic Significance of the Knapsack Problem. Luke J. O'Connor and Jennifer Seberry. Aegean Park Press, 1988.

On Poe and cryptanalysis

"A Few Words on Secret Writing." Edgar Allan Poe, in *Graham's Magazine*, 19, July 1841, pp. 33–38.

"Edgar Allan Poe, Cryptographer." William Friedman, in *American Literature*, 8, November 1936, pp. 226–280.

"What Poe Knew About Cryptography." William Wimsatt, Jr., in *Publications of the Modern Language Association*, 58, 1945, pp. 754–779.

"Poe's Challenge Cipher Finally Broken." Brian Winkel, in *Cryptologia*, 1, January 1977, pp. 93–96. For solution and comments on how they were obtained see the same journal, 1, October 1977, pp. 318–325.

News reports

"Cryptic Reaction." Richard Shaffer, in *The Wall Street Journal*, June 16, 1978, p. 1.

"An Uncrackable Code?" *Time*, July 3, 1978, pp. 55–56.

"Opening the 'Trapdoor Knapsack.'" Philip Faflick, in *Time*, October 28, 1982.

Articles by Gina Bara Kolata in *Science*: "Computer Encryption and the National Security Agency Connection," July 29, 1977, pp. 438–448; "Cryptography: On the Brink of a Revolution?," August 19, 1977, pp. 747–748; "Cryptology: Scientists Puzzle Over Threat to Open Research, Publication," September 30, 1977, pp. 1345–1349; "Cryptology: A Secret Meeting at IDA," April 14, 1978, p. 184; "New Codes Coming Into Use," May 16, 1980, pp. 694–695; "Prior Restraints on Cryptography Considered," June 27, 1980, pp. 1442–1443; "Testing for Primes Gets Easier," September 26, 1980, pp. 1503–1504; "Cryptographers Gather to Discuss Research," November 1981, pp. 646–647; "Another Promising Code Falls," December 16, 1983, p. 1224.

Nontechnical articles

"The New Unbreakable Codes: Will They Put NSA Out of Business?" Deborah Shapley, in *The Washington Post Outlook*, Section B1, July 9, 1978.

"The Mathematics of Public-Key Cryptography." Martin Hellman, in *Scientific American*, August 1979, pp. 146–157.

"Unbreakable Code." Roger Rapoport, in *Omni*, September 1980, pp. 84–86, 92.

"Safety in Numbers." George Davida, in *The Sciences*, July/August 1981, pp. 9–14.

"Cryptology: From Caesar Ciphers to Public-Key Cryptosystems." Dennis Luciano and Gordon Prichett, in *The College Mathematics Journal*, 18, January 1987, pp. 2–17.

Advanced articles

"New Directions in Cryptography." Whitfield Diffie and Martin Hellman, in *IEEE Transactions of Information Theory*, November 1976, pp. 644–654.

"A Method of Obtaining Digital Signatures and Public-Key Cryptosystems." Ronald Rivest, Adi Shamir and Leonard Adleman, M.I.T. Laboratory for Computer Science, Technical Memo 82, April 1977. Reprinted in *Communications of the ACM*, 21, February 1978, pp. 120–126.

"Preliminary Comments on the M.I.T. Public-Key Cryptosystem." Gustavus Simmons and Michael Norris, in *Cryptologia*, 1, October 1977, pp. 406–414. See Rivest's reply in the same journal, 2, January 1978, pp. 62–65.

"Secure Communications Over Insecure Channels." R. C. Merkle, in *Communications of the ACM*, 21, April 1978, pp. 294–299.

"Hiding Information and Signatures in Trapdoor Knapsacks." R. Merkle and M. Hellman, in *Transactions of Information Theory*, September 1978, pp. 525–530.

"Cryptology: The Mathematics of Secure Communication." G. J. Simmons, in *Mathematical Intelligencer*, 1, 1979, pp. 233–246.

"Privacy and Authentication: An Introduction to Cryptography." Whitfield Diffie and Martin Hellman, in *Proceedings of the IEEE*, 67, March 1979, pp. 397–427.

"Secrecy, Authentication, and Public-Key Systems." Ralph Charles Merkle, Technical Report 1979-1, Information Systems Laboratory, Stanford University, June 1979.

"Symmetric and Asymmetric Encryption." Gustavus Simmons, in *Computing Surveys*, 11, December 1979, pp. 305–330. Bibliography has 66 references.

"Error-Correcting Codes and Cryptography." N. J. A. Sloane, in *The Mathematical Gardner*. Prindle, Weber, and Schmidt, 1981.

"A Polynomial Time Algorithm Testing for Breaking the Basic Merkle-Hellman Cryptosystems." A. Shamir, in *Proceedings of the 23rd Annual Symposium of the Foundations of Computer Science*, 1982, pp. 145–152.

"On Breaking the Generalized Knapsack Public-Key Cryptosystem." L. M. Adleman, in *Proceedings of the 15th ACM Symposium on Theory of Computing*, 1983, pp. 402–412.

"How to Exchange (Secret) Keys." Manuel Blum, in *ACM Transactions on Computer Systems*, 1, May 1983, pp. 175–193.

"Integer Programming and Cryptography." H. W. Lenstra, Jr., in *Mathematical Intelligencer*, 6, 1984, pp. 14–19.

"Proof Checking the RSA Public-Key Encryption Algorithm." Robert Boyer and J. Strother Moore, in *The American Mathematical Monthly*, 91, March 1984, pp. 181–189.

"Cryptology." Ronald Rivest, in the *Handbook of Theoretical Computer Science*, Chapter 13, 1988. An excellent overview of the current revolution in cryptography. The bibliography runs to more than 170 references.

On the DES system

"Assessment of the National Bureau of Standards Proposed Federal Data Encryption Standard." Robert Morris, N. J. A. Sloane and A. D. Wyner, in *Cryptologia*, 1, 1977, pp. 281–306.

"Exhaustive Cryptanalysis of the NBS Data Encryption Standard." W. Diffie and M. E. Hellman, in *Computer*, 10, June 1977, pp. 74–84.

"DES Will Be Totally Insecure Within Ten Years." M. E. Hellman, in *IEEE Spectrum*, 16, July 1979, pp. 32–39.

On zero-knowledge proofs

"Keeping Secrets: How to Prove a Theorem So That No One Else Can Claim It." Ivars Peterson, in *Science News*, 130, August 30, 1986, pp. 140–141.

"Zero-Knowledge Proofs." Joe Buhler, in *Focus* (newsletter of the American Mathematical Association), 6, October 1986, pp. 1, 6–7.

"A New Approach to Protecting Secrets is Discovered." James Glieck, in the *New York Times*, February 17, 1987, pp. 17–18.

"Brief U.S. Suppression of Proof Stirs Anger." *New York Times*, February 17,

Contemporary Cryptography. Gustavus Simmons. IEEE Press, 1992.

Public-Key Cryptography. T. Beth, M. Frish, and G. J. Simmons (eds.) Springer-Verlag, 1992.

"Cipher Probe." William Bulkeley, in *The Wall Street Journal,* April 28, 1994, page 1ff.

"Suddenly, Number Theory Makes Sense to Industry." Fred Guterl, in *Business Week,* June 20, 1994, pp. 172–74.

"Lost in Kafka Territory." *U. S. News,* April 3, 1995, pp. 32–33.

"The Encryption Wars." Steven Levy, in *Newsweek,* April 24, 1995, pp. 55–56.

"Whitfield Diffie," an interview, in *Omni,* Winter 1995, pp. 87–93.

"Confidential Communication on the Internet." Thomas Beth, in *Scientific American,* December 1995, pp. 88–91.