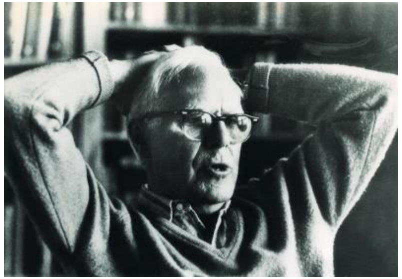
The RSA Cryptosystems (10)

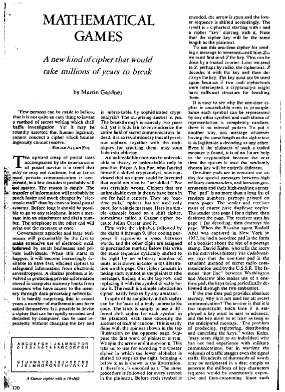
- The RSA cryptosystem is **asymmetric**: it is difficult to calculate the **Decryption Key** D from the **Encryption Key** E.
- Using this property, we can design the system to authenticate the messages (**Digital Signature**).

Interlude: The Magic Words are Squeamish Ossifrage (1)

- In 1977, just after Rivest, Shamir, and Adleman invented RSA, Gardner wrote a column in *Scientific American*, and gave a challenge to readers.



Martin Gardner
(1914-2010)



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

120

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 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

https://en.wikipedia.org/wiki/Martin_Gardner
Scientific American 237 (2), 120-124, Aug 1977.

Interlude: The Magic Words are Squeamish Ossifrage (2)

- It is to find **prime numbers** P,Q s.t. P×Q = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
- A secret message was encrypted using this number by RSA.
- At that time, it was estimated to take 40×1000000000000000 years to find P,Q. (The universe is 13800000000 years old.)

Interlude: The Magic Words are Squeamish Ossifrage (3)

- In 1994, the problem was solved by more than 600 volunteers in 8 months.

  P=3490529510847650949147849619903898133417764638493387843990820577

  Q=32769132993266709549961988190834461413177642967992942539798288533

- The secret message was

  THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Bearded vulture (ossifrage)

https://en.wikipedia.org/wiki/Bearded_vulture