"Electronics, Information and Communication" field

Achievement : Contribution to information security through pioneering research on cryptography

Dr. Adi Shamir (Israel)

Born: July 6, 1952 (Age: 64, Nationality: Israel)
Professor, Weizmann Institute of Science

Summary

The advent of open digital networks, namely the Internet, has enabled us to lead a convenient lifestyle like never before. Such comfort has been made possible thanks to security measures preventing the theft and manipulation of valuable information. It is Dr. Adi Shamir who proposed many of the underlying concepts in information security and developed a series of practical solutions.

Information in digital networks is coded in binary digits. Utilizing mathematical methodology, Dr. Shamir has invented and proposed numerous techniques, such as the innovative "RSA cryptosystem," the "secret sharing scheme" which ensures secrecy by breaking up classified information into parts and dispersing it among several participants, the "identification scheme" with which individuals can be identified without revealing secret information and the generic "differential cryptanalysis" which deciphers many common key cryptosystems.

Dr. Shamir has also made a significant breakthrough in the research of side-channel attacks which decipher code by monitoring the physical information of the computer carrying out encryption, such as power consumption and noise.

Co-developing the first practical public-key cryptography with two MIT researchers

Cryptography plays an important role in our lives, but for a long time, it was primarily used by specific groups in society such as the government and the military. In such cases, the same cryptographic key was used for both encryption and decryption, and was secretly shared among specific individuals in the group. However, as open digital networks emerged and a large number of unspecified users began to exchange information, the need for a new cryptosystem arose to overcome major issues of safety surrounding the distribution and sharing of cryptographic keys.

In 1976, Stanford University researchers Dr. Whitfield Diffie and Dr. Martin Hellman proposed a new cryptosystem called the "public key cryptography." The system has two types of keys, the encryption key which is open to the public, and the decryption key which is kept private. This scheme allows a large number of unspecified people to send secret information encrypted with a public key, which can only be decrypted by the intended recipient. This enables secure transactions, such as shopping over the internet with a credit card.

Its first practical realization, the "RSA cryptosystem," was co-developed in 1977 by three young researchers at MIT (Massachusetts Institute of Technology), namely Dr. Ron Rivest, Dr. Adi Shamir, and Dr. Leonard Adleman.

Intrigued by the proposal of public key cryptography, Dr. Rivest and Dr. Shamir explored encryption methods using various mathematical techniques. Joining midway through the research, Dr. Adleman searched for flaws that could lead to decryption. After numerous trials, they finally succeeded with their 43rd iteration, and named it the RSA cryptosystem taking the first letter of the three doctors' names.

The essential basis of this cryptosystem lies in the difficulty in the prime factorization of very large numbers (the product of two prime numbers). The product of two prime numbers is publicly released as the encryption key. In order to uncover the decryption key, one needs to perform prime factorization on the encryption key, and identify the two prime numbers. The product of two prime numbers used in today's RSA cryptosystem expressed in binary is between 2^{2048} and 2^{4096}, much greater than the total number of atoms in a galaxy, which is 2^{223}. Even a supercomputer would be unable to compute this in 10 thousand years.

The RSA cryptosystem can also be used as a signature mechanism. A message encrypted using the decryption key can in turn be decrypted using the encryption key, allowing anyone to verify the signatory as the one with the decryption key.

The invention of the secret sharing scheme which protects information from disasters

Information dispersal is crucial for the secure storage of important data. In 1979, Dr. Shamir was the first to propose the "secret sharing scheme," which specifies the dispersal method that ensures the security of information depending on the extent of dispersed information leakage. This was achieved using the polynomial method.

Based on the fact that a straight line is a first degree polynomial, and a parabola is a second degree polynomial, secret information is represented as points on the polynomial. Points other than the secret information are dispersed and stored. By doing so, a first degree polynomial requires two pieces of dispersed information, and that of the second degree requires three pieces of dispersed information to recover the secret information. This is because two points are sufficient to draw a straight line with accuracy, and three points for a parabola. Similarly, for a polynomial of order k, the secret information can be recovered by gathering k+1 pieces of dispersed information. By dispersing information into k+1 pieces or more, up to k pieces of information can be stolen without it being disclosed, and even if several of them are damaged, it can be restored as long as k+1 pieces remain safe. By using this scheme, valuable data can be dispersed according to its intended purpose. As an earthquake countermeasure, for example, information can be dispersed across three separate locations around the country. Even if information in one of the locations is destroyed in an earthquake, data can be recovered using information from the other two locations.

In addition, Dr. Shamir invented the "visual secret sharing scheme." It involves splitting an image into two or more sandstorm-like patterns, which, when overlapped, reveal the original image. The separated images are expressed as light and dark dots that, when overlapped, manifests as light-light, light-dark or dark-dark overlay, thereby reproducing the original image.

Following Dr. Shamir's proposal of the "secret sharing scheme," a diverse range of variants has been studied by numerous researchers. Besides being adopted for practical use, this scheme has also been applied to other cryptographic technology, thereby contributing enormously to the advancement of cryptographic technology research.

An identification scheme that does not reveal any secret information

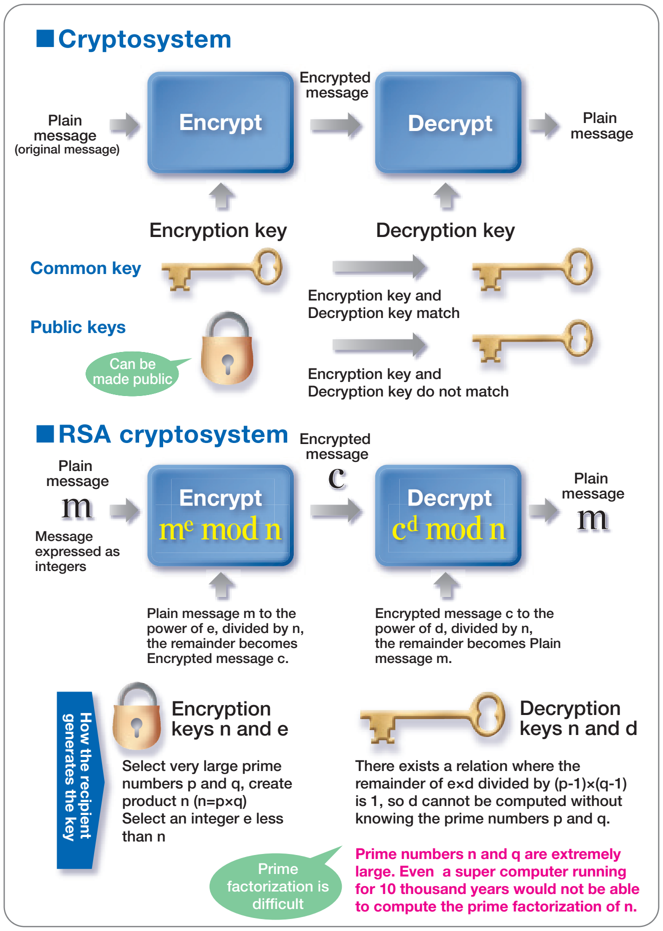
In the physical world, IDs such as a driver license must be presented in order to prove one's identity. In digital networks, however, presenting secret information such as a password poses a risk of it being stolen, which could lead to identity theft.

In 1986, Dr. Shamir developed an "identification scheme," which proves one's possession of authentic secret information during a transaction without revealing any of it to the other party. Based on the mathematical theory of quadratic residue, it is a magnificent achievement both academically and practically, and has been adopted by satellite broadcasting services in billing systems that guarantee the authenticity of its users.

The discovery of a generic method for decrypting common-key cryptosystems

Advancement in cryptographic technology requires not only the development of new technology but also the discovery of flaws in existing technology. The RSA cryptosystem by Dr. Shamir's group was developed to hold up against Dr. Adleman's deciphering tests. Dr. Shamir himself studied the risk of illegitimate deciphering in great depth and has made important suggestions on the topic.

In 1990, Dr. Shamir demonstrated that many common key cryptosystems could be deciphered, by analyzing the statistical differences in the differential values of two encrypted messages which results in parts of


■Cryptosystem
Plain message (original message)
Encrypt
Encrypted message
Decrypt
Plain message
Encryption key
Decryption key
Common key
Encryption key and Decryption key match
Public keys
Can be made public
Encryption key and Decryption key do not match
■RSA cryptosystem
Plain message
m
Message expressed as integers
Encrypt
m^e mod n
Encrypted message
c
Decrypt
c^d mod n
Plain message
m
Plain message m to the power of e, divided by n, the remainder becomes Encrypted message c.
Encrypted message c to the power of d, divided by n, the remainder becomes Plain message m.
How the recipient generates the key
Encryption keys n and e
Select very large prime numbers p and q, create product n (n=p×q) Select an integer e less than n
Decryption keys n and d
There exists a relation where the remainder of e×d divided by (p-1)×(q-1) is 1, so d cannot be computed without knowing the prime numbers p and q.
Prime factorization is difficult
Prime numbers n and q are extremely large. Even a super computer running for 10 thousand years would not be able to compute the prime factorization of n.

the encryption process canceling each other out.

Many common key cryptosystems encrypt information by the repeated application of simple encryption process, and are therefore prone to such a decryption method. Dr. Shamir went on to prove that it is possible to decipher the DES (Data Encryption Standard), adopted by the National Bureau of Standards (NBS, today's NIST) in 1977 as the world's first encryption standard for commercial transaction, if only eight or so iterations of the encryption processes are performed.

In practice, DES was never cracked as it had been encrypting information 16 times over. This discovery, however, spurred the development of a safer cryptosystem and led to NIST's adoption of a new encryption standard in 2000.

Deciphering encryption using a smartphone placed beside a PC

Deciphering information by analyzing the activities of the encryption and decryption program based on fluctuations in the computer's physical information, such as power consumption and machine noise, is called a side-channel attack. From an early stage, Dr. Shamir focused on side-channel attacks and made numerous breakthroughs.

In 2014, Dr. Shamir demonstrated that it is possible to break the RSA encryption, developed by him and his colleagues, by analyzing the machine noise picked up by a smartphone placed beside the computer. Such findings hold important significance for the future design of secure systems including the hardware.

As described, Dr. Shamir, through 40 years of research, has transformed cryptography from a minor technology for the few to the academic discipline of "cryptology."

In an era in which the rise of open digital networks has enabled the people of the world to freely exchange information, Dr. Shamir has consistently pioneered the frontiers of information security research and created new research trends. With the emergence of intelligent computing such as A.I., great anticipation is building around the future of Dr. Shamir's research.