Euler and cryptology

Euler and cryptology

Euler was active and innovative in number theory. Number theory is famous for its purity and apparent lack of applications, but in fact number theory is extremely useful. For example, modern cryptography is strongly linked to Euclid, Fermat and Euler theorems.

What is cryptography?

Cryptography is the study of message secrecy, now a branch of information theory: the mathematical study of information and its transmission from place to place. It is a central contributor to information security, authentication, and access control. A main purpose is to hide the meaning of messages, e.g. in computer, network security, the security of ATM cards, passwords, or e-commerce.

It is a very old field of technical study, about 4,000 years old. It was purely a method of encryption with pen and paper until the invention in the early 20th century of complex mechanical and electromechanical machines, such as the sophisticated Enigma rotor machine.

Euler's totient function

In number theory, Euler's totient $\varphi(n)$ of a positive integer n is defined to be the number of positive integers less than or equal to n and coprime to n. For example, $\varphi(8) = 4$ since the four numbers 1, 3, 5 and 7 are coprime to 8. The function φ so defined is Euler's totient function. Euler's totient function is also called Euler's φ function.

Euler's theorem

In number theory, Euler's theorem (also known as the Fermat-Euler theorem or Euler's totient theorem) states that if n is a positive integer and a is coprime to n, then

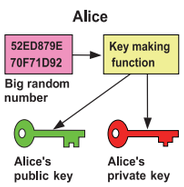
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

where $\varphi(n)$ is Euler's totient function and "mod" denotes the congruence relation.

The theorem may be used to easily reduce large powers modulo n. For example, consider finding the last decimal digit of 7^{222}, i.e. $7^{222} \pmod{10}$. Note that 7 and 10 are coprime, and $\varphi(10) = 4$. So Euler's theorem yields $7^4 \equiv 1 \pmod{10}$, and we get $7^{222} \equiv 7^{4\cdot 55 + 2} \equiv (7^4)^{55} \cdot 7^2 \equiv 1^{55} \cdot 7^2 \equiv 49 \equiv 9 \pmod{10}$.

Public key cryptography

Public key cryptography is a form of cryptography to allow users to communicate securely without having prior access to a shared secret key. This is done by using a related pair of cryptographic keys, the public key and the private key . What has been encrypted by one key can only be decrypted by the other key.



The private key is kept secret, while the public key may be widely distributed. In a sense, one key "locks" a lock, while the other is required to unlock it. In high quality algorithms, the private key of a pair cannot be deduced given the public key.

Imagine that Alice sends a secret message to Bob through the public mail, then Bob sends a secret reply. With a symmetric key system, Alice first puts the secret message in a box, locks it with a key and sends it to Bob by mail. Bob then opens the box with the same key that he gets via another channel.

RSA

RSA involves a public and private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and $\varphi = (p-1)(q-1)$.
3. Choose an integer e, $1 < e < \varphi$, such that $\gcd(e, \varphi) = 1$.
4. Compute the secret exponent d, $1 < d < \varphi$, such that $ed \equiv 1 \pmod{\varphi}$.
5. The public key is (n, e) and the private key is (n, d). The values of p, q, and φ should also be kept secret.

- n is known as the modulus
- e is known as the public exponent
- d is known as the secret exponent

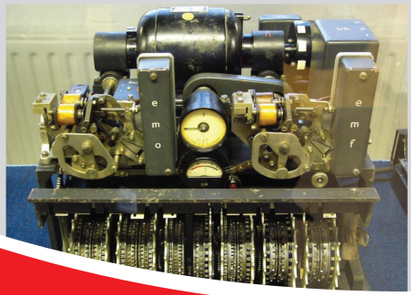
Johann Friedrich Euler (1741-1800): mathematician, cryptologist, cousin of Leonhard Euler

During the latter part of the 18th century, mathematicians started to study and develop cryptology, thanks to Euclid, Fermat and Euler theorems. Johann Friedrich Euler, mathematician and cryptologist at the Court of Netherlands, showed a marked ability to put into practice new principles, including very likely his cousin's discoveries. He started his cryptologist career in 1782; he constructed codes and ciphers on behalf of the Stadholder in his first years in The Hague. The code book he published, with construction of an extensive, two-part code, comprising of roughly 4000 items, was intended for encryption of correspondence between the Stadholder and some of the Republic's emissaries abroad.

In many fields of security, Swiss industry is world-leading, for example for highly secure banknotes, passports, etc, including security inks, or electronic cards technology for cashless payments, eTicketing, public transport or parking.

The Ancient Greek scytale, probably much like this modern reconstruction, may have been one of the earliest devices used to implement a cipher.

The German Lorenz cipher machine, used in World War II for encryption of very high-level general staff messages.



The security of ATM transactions relies mostly on the encryption of personal information, required by law in many jurisdictions and is used to prevent fraud. In Switzerland, IBM Zurich Research Laboratory is strongly involved in research in privacy and data protection technology, for example for safe e-commerce. It is the European branch of IBM Research and was its first research center outside the US. It won 2 Nobel Prices.

A picture of the book jacket, "Da Vinci Code".

$$e^{i\pi} + 1 = 0$$

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
State Secretariat for Education and Research

Switzerland.