Reason - A Technical Magazine
Vol. – VIII, 2007 & 2008

HISTORY OF CRYPTOGRAPHY

Satyendra Nath Mandal
Lecturer, Department of IT
Kalyani Govt. Engineering College

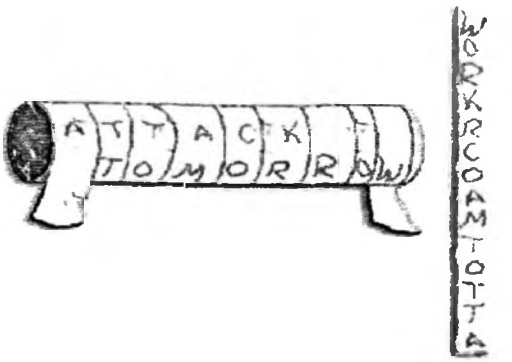
ABSTRACT : Cryptography is an art of science to secure the confidential data. In the present paper, a brief history of the development of cryptography and its recent trends are outlined.

1. TYPICAL CRYPTOGRAPHIC SCENARIO

Alice wants to send a message to Bob in such a way that Eve cannot possibly read it. Assuming A and B cannot keep E from intercepting their communication, A must find a way to disguise the message, plaintext , into ciphertext. The process of turning plaintext into ciphertext is called encryption and its reverse is called decryption.

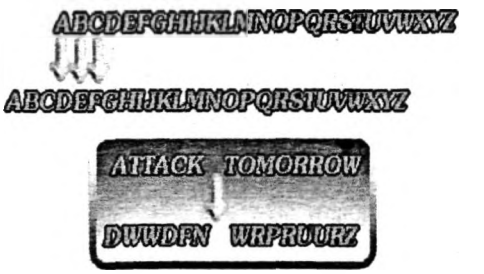
2. ANCIENT CRYPTOGRAPHY

Early encryptions were based on two operations: permutations and substitutions of characters. These two methods of encryption are still employed by cryptographers today, albeit in more sophisticated ways!



2.1 PERMUTATIONS

An example of the use of permutations of characters for encryption is the 'scytale' or a stick with a fixed width, used by the Greeks around 6 BC to encrypt their messages. To encrypt the message, the sender would wrap a long piece of paper around the scytale, and then write the intended message in a horizontal manner. This long strip of paper would then be unrolled and sent to the receiver, who would only be able to decrypt the message with a scytale of similar width.



2.2 SUBSTITUTION

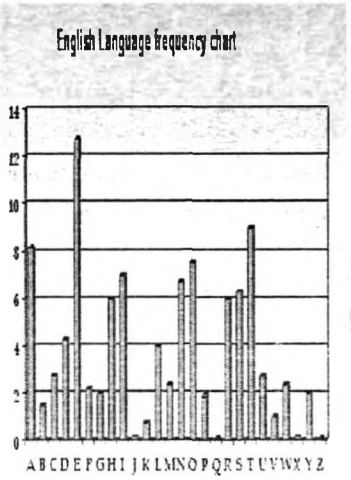
The Caesar shift, used by the Roman army over two thousand years ago, to encrypt communication between troops, is an example of the use of substitution of characters for encryption. The Caesar shift is carried out by shifting all the characters in the message, usually by 3 positions. Hence, the character A would be replaced by D, B by E and so on.

2.3 CRYPTOGRAPHIC KEYS

Encryption methods are usually publicly known, e.g. everyone knows the principle behind the Caesar cipher. However, the encryption has a flexible component known as the key, which is kept secret. The Caesar cipher with 25 letters admits any shift between 1 and 25, so it has 25 possible keys (or 26 keys if you allow the zero shift). The most general form of one-to-one substitution allows the ciphertext alphabet to be any rearrangement of the plaintext alphabet, so it has 26! or 403,291,461,126,605, 635,584,000,000 keys. And yet, ciphers based on one-to-one substitutions, also known as monoalphabetic ciphers, can be easily cracked!

3. ANCIENT CRYPTANALYSIS

It is not known who pioneered cryptanalysis (codebreaking). The earliest essay on the subject is by the 9th century polymath from Baghdad, al-Kindi (800-873AD), also known as the philosopher of the Arabs. Al-Kindi noticed that if a letter in a plaintext is replaced with a different letter or symbol in a ciphertext, the new letter will take on all the characteristics of the original one. A simple substitution cipher cannot disguise certain features of the plaintext, such as the relative frequencies of the different characters. Take the English language: the letter E is the most common letter, accounting for 13% of all letters. So, if E is replaced by a symbol X, then X will account for 13% of symbols in the encrypted message, thus a cryptanalyst can work out that X actually represents E.



The Adventure of the Dancing Men by Arthur Conan Doyle gives an example of monoalphabetic ciphers and describes how it is broken by frequency analysis

3.1 LIPOGRAMS

Some writers defy the natural frequency of letters by creating LIPOGRAMS: "That's right, this is a lipogram - a book, paragraph or similar thing in writing that fails to contain a symbol, particularly that symbol fifth in rank out of 26 (amidst 'd' and 'f') and which stands for a vocalic sound such as that in 'kiwi'. I won't

bring it up right now, to avoid spoiling it..." The most famous lipogram is probably the French novel *La Disparition* by George Perec, 85000 words without the letter *e*. English translator, Gilbert Adair, in *A Void*, succeeded in avoiding the letter *e* as well.

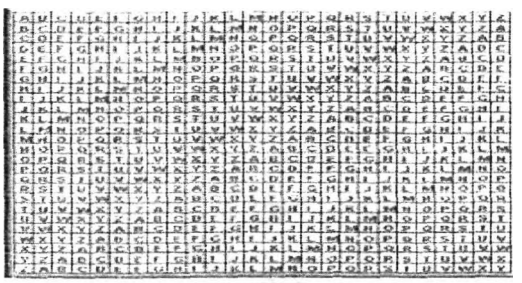
3.2 POLYALPHABETIC CIPHERS

Leone Battista Alberti (1404-1472), the Renaissance architect, invented a device based on two concentric discs that simplified encryption and decryption of Caesar ciphers. The substitution - i.e. the relative shift of the two alphabets - is determined by the relative rotation of the two disks.Alberti also considered changing the substitution during the encryption, by turning the inner disc. It is believed that this is how he discovered the so-called polyalphabetic ciphers, which are based on superpositions of Caesar ciphers with different shifts.

Alberti Disk

In polyalphabetic ciphers the key can denote a sequence of shifts e.g. (7,14,19) , which means shift the first letter in the message by seven, the second letter by fourteen, the third by nineteen, the fourth again by seven, the fifth by fourteen, the sixth by nineteen, and so on repeating the shifts (7,14,19) throughout the whole message. A convenient way to generate and to memorise such a key is to use a keyword. If we put A=0, B=1, C=2...H=7....Z=25, then the key (7,14,19) can be remembered as the keyword HOT. The encryption and decryption is then much simplified if we use the Vigenere Square, shown below, which has a plaintext alphabet followed by 26 cipher alphabets, each one shifted by one more letter with respect to the previous one. The keyword HOT encrypts the plaintext QUANTUM into ciphertext XITUHNT.

The idea to use a sequence of substitution ciphers in turn was re-invented several times, partly because it was such an obvious complication of the Caesar cipher, and partly because the sixteenth century Europe, Italy in particular, was a place of turmoils, intrigues and struggles for political and financial power. Needless to say, this cloak-and-dagger atmosphere was ideal for cryptology to flourish. The three important contributors to the field at the time were Johannes Trithemius (1462-1516), Blaise de Vigenere (1523-1596), and Giovanni Battista Della Porta (1535-1615). All three of them designed polyalphabetic ciphers which were difficult to break, for at least another 200 years. The first systematic method of breaking polyalphabetic ciphers was designed by Charles Babbage (1791-1871) in 1854. The method is focused on the length of the key or the keyword - if the key has n letters then every nth symbol in the ciphertext is encrypted with the same key. Thus, the ciphertext can be divided into n subtexts, and each then cracked by frequency analysis.



Vigenere Square

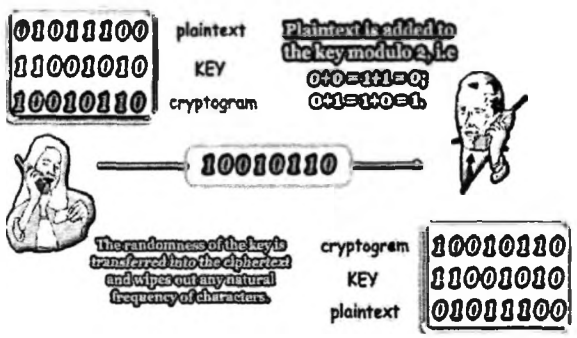
The title page illustration from Johannes Trithemius' 1518 "Polygraphiae libri sex" shows the author wearing his Benedictine habit and kneeling to present his book to the Holy Roman Emperor Maximilian.

In the 1920s electromechanical technology led to the development of rotor machines, in which an encrypting sequence with an extremely long key period could be generated, by rotating a sequence of rotors. A notable achievement of cryptanalysis was the breaking of the Enigma in 1933.In the winter of 1932, Marian Rejewski, a twenty-seven year old cryptanalyst working in the Cipher Bureau of the Polish Intelligence Service in Warsaw, Poland, mathematically determined the wiring of the Enigma's first rotor. From then on, Poland was able to read thousands of German messages encrypted by the Enigma Machine. During WW2 further spectacular advances in breaking the Enigma ciphers were made by Alan Turing and his colleagues at Bletchley Park.

ENIGMA

3.3 TOWARDS A PERFECT CIPHER - ONE-TIME PAD (VERNAM CIPHER)

Longer keys make polyalphabetic ciphers more secure. The extreme case is the One Time Pad, where the key is the same length as the plaintext. If the key is also secure, truly random, and never reused, the cipher is unbreakable! The One Time Pad, also known as the Vernam Cipher, was developed By Gilbert Vernam of AT&T in 1918. As far as we know, this is the only totally secure cipher



4. KEY DISTRIBUTION PROBLEM

With the discovery of the Vernam Cipher, it was possible now to produce a totally secure cipher. However, the problem of key distribution was still a problem. How do we distribute the cryptographic key securely? Especially so since the every Vernam cipher should only be used once, and new random keys have to be produced each time. There are two solutions to this problem

- Public-Key Cryptography
- Quantum Cryptography

RESOURCES AND LINKS

- Greg Goebel: "Codes, Ciphers and Codebreaking" — An excellent online document on codes and ciphers.
- Oliver Pell : "Cryptology" — A prize winning essay on cryptology.
- Ron Hipscham : "The Secret Language" .
- "History of Cryptology" — Article on the history of cryptology on Resonance Publications
- Heather Blatt : "Secret Writing in the Middle Ages and Renaissance" .
- The Cypher Research Laboratories, Australia : "A Brief History of Cryptography" .
- "Navajo Code Talkers: World War II Fact Sheet" — US Navy's website detailing the history of Navajo Code Talkers who were used during WWII.
- "Enigma Simulator" — Simulators of the enigma machine for all platforms.