A Brief History of Cryptography & Cryptanalysis (Cryptology)

- Cryptology is the study of both cryptography, the use of messages concealed by codes or ciphers, and cryptanalysis, or the breaking of coded messages. It is nearly as old as civilization itself.

- Ever since we crawled out of the caves mankind has been trying to conceal information in written form once forms or writing were developed.

- Many such examples that survive in stone inscriptions and papyruses illustrate that many ancient civilisations including the Egyptians, Hebrews and Assyrians all developed cryptographic systems.

- Early examples of cryptology can be found in the work of Mesopotamian, Egyptian, Chinese, and Indian scribes.

- In those four cradles of civilization, which emerged during the period between 3500 and 2000 BC, few people could read and write, therefore, written language was a secret code in itself.

- Further concealment of meaning behind opaque hieroglyphs, cuneiform (system of writing developed by the ancient Sumerians of Mesopotamia), or ideograms served to narrow the intended audience even further.

Ancient Cryptology

- The first known evidence of the use of secret writing was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt, where an unusual set of hieroglyphic symbols were used to replace commonly used ones.

- The intent was not to hide the message but perhaps to change its form in a way which would make it recognizable to a select few. In that sense it is more of a transformation of the original text.

- "Arthshashtra", a classic work on statecraft written by Kautalya, describes the espionage service in India and mentions giving assignments to spies in "secret writing".

- The Greeks were therefore the inventors of the first transposition cipher and in the fourth century BC the earliest treatise on the subject was written by a Greek, Aeneas Tacticus, as part of a work entitled *On the Defence of Fortifications*.

- Another Greek, Polybius later devised a means of encoding letters into pairs of symbols using a device known as the *Polybius checkerboard* which contains many elements common to later encryption systems.

- The Polybius checkerboard consists of a five by five grid containing all the letters of the alphabet. Each letter is converted into two numbers, the first is the row in which the letter can be found and the second is the column. Hence the letter A becomes 11, the letter B 12 and so forth.

- In addition to the Greeks there are similar examples of primitive substitution or transposition ciphers in use by other civilisations including the Romans.

- The first recorded use of cryptography for correspondence was by the Spartans who (as early as 400 BC) employed a cipher device called a "scytale" to send secret communications between military commanders.

- The scytale consisted of a tapered baton around which was wrapped a piece of parchment inscribed with the message. Once unwrapped the parchment appeared to contain an incomprehensible set of letters, however when wrapped around another baton of identical size the original text appears.

- Around 100 BC, Julius Caesar developed a form of encryption to convey secret messages to his army generals posted in the war front. This substitution cipher, known as Caesar cipher, is perhaps the most mentioned historic cipher in academic literature.

- In a substitution cipher, each character of the plain text (plain text is the message which has to be encrypted) is substituted by another character to form the cipher text (cipher text is the encrypted message).

- The variant used by Caesar was a shift by 3 cipher. Each character was shifted by 3 places, so the character 'A' was replaced by 'D'; 'B' was replaced by 'E'; and so on. The characters would wrap around at the end, so 'X' would be replaced by 'A'.

Medieval Cryptology

- The Arabs were the first people to clearly understand the principles of cryptography and to elucidate the seminal versions of cryptanalysis.

- They devised and used both substitution and transposition ciphers and discovered the use of letter frequency distributions in cryptanalysis.

- Arab scholars pioneered cryptanalysis, the solving of ciphers or codes without the aid of a key, from the eighth century onward. In 1412, al-Kalka-shandi published a treatise (in his encyclopaedia *Subh al-a'sha*) in which he introduced the technique, later made famous to popular audiences by Edgar Allan Poe in "The Gold Bug," of solving a cipher based on the relative frequency of letters in the language.

- European cryptography dates from the Middle Ages during which it was developed by the Papal and Italian city states. The earliest ciphers involved only vowel substitution (leaving the consonants unchanged).

- By this time, cryptology had begun to advance in Europe, where the Italian city states used secret codes for their diplomatic messages in the fourteenth century. Messages were carried on horseback, and even in peacetime, the roads of Europe were plagued with highway robbers, so secrecy in communication was of the utmost importance.

- Progress in mathematical learning from the twelfth century onward aided these advances. In the early thirteenth century, Italian mathematician Leonardo Fibonacci introduced the Fibonacci sequence, wherein each number is the sum of the previous two: 1, 1, 2, 3, 5, 8, and so on.

- Fibonacci's sequence would prove highly influential in cryptology: even in the late twentieth century, some cryptologic systems relied on an electronic machine called a Fibonacci generator, which produced numbers in a Fibonacci sequence.

- Circa 1379 the first European manual on cryptography, consisting of a compilation of ciphers, was produced by Gabriele de Lavinde of Parma, who served Pope Clement VII.

- This manual contains a set of keys for correspondents and uses symbols for letters and nulls with several two character code equivalents for words and names.

- The first brief code vocabularies, called nomenclators, were expanded gradually and for several centuries were the mainstay of diplomatic communications for nearly all European governments.

The Early Modern Era (1500–1900)

- In 1470 Leon Battista Alberti described the first cipher disk in *Trattati in cifra* and the *Traicté de chiffres*, published in 1586 by Blaise de Vigernère contained a square table commonly attributed to him as well as descriptions of the first plaintext and ciphertext autokey systems.

- By the late fifteenth century, Alberti published a work in which he introduced the idea of a cipher disk. The latter is a device for encoding and decoding messages by use of concentric wheels imprinted with alphabetic and numeric characters.

- During the 16th century, Vigenere designed a cipher that was supposedly the first cipher which used an encryption key. In one of his ciphers, the encryption key was repeated multiple times spanning the entire message, and then the cipher text was produced by adding the message character with the key character modulo 26.

- The German monk Trithemius developed a table in which each row contained all the letters of the alphabet, but each successive row was shifted over by one letter. The first letter of plain text would be encrypted using the first line, the second letter using the second line, and so on.

- In the late 1500s, Blaise de Vigenère adapted the Trithemius table for his own table, which in the twentieth century became the basis for the widely used data encryption standard, or DES in the 1980s and 1990s.

- By the eighteenth and early nineteenth centuries, cryptography had become widely used in Europe, where governments employed special offices called "black chambers" to decipher intercepted communications.

- In America, Thomas Jefferson developed an early cipher wheel, and in the 1840s, Samuel F. B. Morse introduced a machine that would have a vast impact on cryptology: the telegraph.

- Up to this time, all encoded or enciphered communication had been written and carried by hand, and the telegraph marked the first means of remote transmission. It also employed one of the most famous codes in the world, the Morse code, and helped influence widespread popular interest in cryptography.

- In the 1850s, Charles Wheatstone and Lyon Playfair introduced the Playfair system, which used a Polybius square and encrypted letters in pairs. This pairing made deciphering more difficult, since it was less easy to see how frequently certain letters appeared.

- Despite these advances of the era, cryptography was still far from advanced during the American Civil War. The Confederacy was so disadvantaged in the field of cryptanalysis that its government sometimes published encrypted Union messages in newspapers, appealing for help from readers in deciphering them.

The Twentieth Century

- In the early twentieth century, another invention, long distance wireless radio transmission, had a profound effect on cryptography by greatly improving the capacity of senders to transmit messages to remote areas.

- World War I marked a watershed in cryptography. Not only was it the first major conflict in which radio was used, it was the last in which a great power failed to employ cryptographic communications.

- On the Eastern Front, the Russians sent plaintext messages that were easily interpreted by Russian-speaking intelligence officers on the German and Austrian side, leading to a massive victory for the Central Powers at Tannenberg in 1914.

- The war also marked the debut of the Germans' ADFGX cipher, which was so sophisticated that French cryptanalysts only deciphered it for one day, after which the Germans again changed the key.

- During this time the British cryptologists also began to emerge when the British signal intelligence cracked the German cipher, and intercepted a message from German foreign minister Arthur Zimmermann to the Mexican president, promising to return territories Mexico had lost to the United States in the Mexican War if the country attacked the United States. Informed of the Zimmermann telegram, President Woodrow Wilson declared war on Germany.

- At the start of the 19th century when everything became electric, Hebern designed an electro-mechanical contraption which was called the Hebern rotor machine. It uses a single rotor, in which the secret key is embedded in a rotating disc.

- The key encoded a substitution table and each key press from the keyboard resulted in the output of cipher text. This also rotated the disc by one notch and a different table would then be used for the next plain text character. This was again broken by using letter frequencies.

- Also in 1917, American engineer Gilbert S. Vernam developed the first significant automated encryption and decryption device when he brought together an electromagnetic ciphering machine with a teletypewriter.

- A year later, Major Joseph O. Mauborgne of the U.S. Army devised the one-time pad, whereby sender and received possess identical pads of cipher sheets that are used once and then destroyed—a virtually unbreakable system.

- It is very true that the most significant advances in Cryptography and Cryptanalysis were driven by the first two world wars.

Cryptography During The Two World Wars

- In the 1920s the maturing of mechanical and electromechanical technology combined with telegraphy and radio brought about a revolution in cryptodevices - the development of rotor cipher machines.

- The concept of the rotor had been anticipated in the older mechanical cipher disks however it was an American, Edward Hebern, who recognised that by hardwiring a monoalphabetic substitution in the connections from the contacts on one side of an electrical rotor to those on the other side and cascading a collection of such rotors, polyalphabetic substitutions of almost any complexity could be produced.

- Hebern tried to sell his idea to the U.S. Navy but the Navy rejected Hebern's system, which was later purchased by the Japanese and used in World War II. By the time of that war, Hebern had developed Mark II (SIGABA), which became the most secure U.S. cipher system during the conflict.

- At almost the same time as Hebern was inventing the rotor cipher machine in the United States, European engineers such as Hugo Koch (Netherlands) and Arthur Scherbius (Germany) independently discovered the rotor concept and designed the precursors to the most famous cipher machine in history - the German Enigma machine which was used during World War 2.

- These machines were also the stimulus for the TYPEX, the cipher machine employed by the British during World War 2. The United States introduced the M-134-C (SIGABA) cipher machine during World War 2.

- The Japanese cipher machines of World War 2 have an interesting history linking them to both the Hebern and the Enigma machines.

- After Herbert Yardley, an American cryptographer who organised and directed the U.S. government's first formal code-breaking efforts during and after the first world war, published *The American Black Chamber* in which he outlined details of the American successes in cryptanalysis of the Japanese ciphers, the Japanese government set out to develop the best cryptographic machines possible.

- The Japanese purchased the rotor machines of Hebern and the commercial Enigmas, as well as several other contemporary machines, for study. In 1930 the Japanese's first rotor machine, code named RED by U.S. cryptanalysts, was put into service by the Japanese Foreign Office.

- However, drawing on experience gained from the cryptanalysis of the ciphers produced by the Hebern rotor machines the U.S. Army Signal Intelligence Service team of cryptanalysts succeeded in breaking the RED ciphers.

- In 1939 the Japanese introduced a new cipher machine, code-named PURPLE by U.S. cryptanalysts, in which the rotors were replaced by telephone stepping switches.

- The greatest triumphs of cryptanalysis occurred during the second world war - the Polish and British cracking of the Enigma ciphers and the American cryptanalysis of the Japanese RED, ORANGE and PURPLE ciphers. These developments played a major role in the Allies' conduct of World War 2.

- The allied cryptologic victories in World War II have long been celebrated in the intelligence community (not to mention in few hundred movies), but the most famous exploit of them all is the cracking of the German Enigma code.

- The Germans' Enigma machine, invented by German electrical engineer Arthur Scherbius around the same time Hebern introduced his device, was a complex creation in which the variable settings of rotors and plugs determined the keys.

- The Enigma machine used 3 or 4 or even more rotors. The rotors rotate at different rates as you type on the keyboard and output appropriate letters of cipher text. In this case the key was the initial setting of the rotors.

- The Enigma machine's cipher was eventually broken by Poland and the technology was later transferred to the British cryptographers who designed a means for obtaining the daily key.

- Solving it was a major victory for the Allies, who kept secret the fact that they had cracked the system so as to keep exploiting it. Cracking of codes also aided victories in North Africa and the Pacific.

- At the same time, American use of "codetalkers" transmitting enciphered messages in the Navajo Indian language made their transmissions indecipherable to the Japanese.

Cryptography In The Modern Age

- Up to the Second World War, the majority of the work on cryptography was for military purposes, usually used to hide secret military information. However, cryptography attracted commercial attention post-war, with businesses trying to secure their data from competitors.

- A quarter-century after the war's end, in the early 1970s, American electrical engineers Martin Hellman and Whitfield Diffie introduced the idea of asymmetric or public-key ciphers, which were extremely hard to crack.

- This led to the development of the RSA algorithm (named for its creators, Rivest, Shamir, and Adelman) at the Massachusetts Institute of Technology in 1977.

- Around the same time in the early 1970's, IBM formed a "crypto group" headed by Horst-Feistel. They designed a cipher called Lucifer. In 1973, the Nation Bureau of Standards (now called NIST) in the US put out a request for proposals for a block cipher which would become a national standard.

- Lucifer was eventually accepted and was called DES or the Data Encryption Standard. In 1997, and in the following years, DES was broken by an exhaustive search attack. The main problem with DES was the small size of the encryption key.
- Given the fact that DES had some 2^{56} possible keys (a number roughly equivalent to a 1 followed by 17 zeroes), it had seemed unbreakable at the time.

- However, by the early 1990s vast increases in the processing speed of computers and distributed processing made it possible for hackers to break DES using "brute-force" methods.

- To guard against these attacks, new Advanced Encryption Standard (AES) algorithms were developed to replace DES.

- In 1997, NIST again put out a request for proposal for a new block cipher. It received 50 submissions. In 2000, it accepted Rijndael, and christened it as AES or the Advanced Encryption Standard.

- Advances in computer technology as well as high-speed data communication over the Internet, have both enabled and necessitated progress in cryptology.

- For example, electronic commerce requires sophisticated encryption systems to protect users' credit card information. Similarly, digital communication via smartphones requires encryption to prevent easy interception of data.

- Developments of the 1990s include Phil Zimmermann's PGP (Pretty Good Privacy) to protect e-mail communications.

- There a multitude of Cryptographic algorithms in use such as Triple-DES, AES, Blowfish, etc. Most of these are variations improvements on DES.

Cryptographic Design Principles

- Security of a “practical” system must rely not on the impossibility but on the computational difficulty of breaking the system (“Practical” => more message bits than key bits)

- The secrecy of your message should always depend on the secrecy of the key, and not on the secrecy of the encryption system. (This is known as Kerckhoffs's principle.)

- When designing ciphers, it is very important to understand and be able to state clearly what the security goals are for the particular cipher.

Kerckhoffs's principle

- Kerckhoffs's principle is one of the basic principles of modern cryptography. The principle goes as follows: A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

- There are six design principles for military ciphers:

    - The system must be practically, if not mathematically, indecipherable.
    - It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
    - Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
    - It must be applicable to telegraphic correspondence.
    - Apparatus and documents must be portable, and its usage and function must not require the concourse of several people.
    - Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

- The second axiom is currently known as Kerckhoffs's principle.

- Kerckhoffs's principle is applied in virtually all contemporary encryption algorithms (DES, AES, etc.). These algorithms are considered to be secure and thoroughly investigated. The security of the encrypted message depends solely on the security of the secret encryption key (its quality).

- Keeping algorithms secret may act as a significant barrier to cryptanalysis, but only if such algorithms are used in a strictly limited circle, which protects the algorithm from being revealed. Most government ciphers are kept secret. Commercial encryption algorithms, released to the market, have mostly been broken quite swiftly.

- Kerckhoffs's principle was reformulated (perhaps independently) by Claude Shannon as "The enemy knows the system" In that form, it is called Shannon's maxim.