The history of practical cryptography from early century bc to modern day essay s...

Cryptography has been in use for centuries to hide messages intended for a specific person or group of persons which are otherwise prohibited or undesirable to be known to others. Its primary use is for security and privacy purposes—that is to ensure secrecy in communications. Some of its early practical uses included military and political communication, and even in private personal endearments.

Cryptography refers to the study of concealing information with the use of mathemathical transformations (Bishop 2). It involves the process of converting the ordinary information, called the plaintext, into a message, called the cyphertext, which would seem unintelligent and unreadable to anyone whose message is not intended to. This process is called encryption. A person who studies or practices cryptography is called a cryptographer.

Decryption is the reverse process of encryption. Cryptographers use secret keys, called cyphers, to encrypt and decrypt messages. Cyphers could be expreesed mathematically as a pair of invertible funtions: f_k, known as the encyphering function which maps froma set S to a set T based on a quantity k called the encyphering key; and g_k, known as the deciphering function which is the inverse of f_k. On the other hand, cryptoanalysis refers to the practice of revealing information hidden by cryptography using analytical and mathematical techniques, without the consent of the cryptographer—that is without the complete knowledge of the cypher. One who practices cryptoanalysis is called a cryptoanalyst, or simply codebreaker (Bishop 2; Singh 10).

The earliest known use of cryptography occurred some 4000 years ago in Egypt where heiroglyphic inscriptions on the tomb of Khnumhotep II were written with a number of unusual symbols to confuse or obscure the meaning of the inscriptions (Cypher Research Laboratories [CYCOM]). In 500-600 BC, Hebrew scribes used a reversed alphabet—that is replacing the first letter of the alphabet with the last, the second with the second to the last, … , and vice versa—known as the atbash cypher, to hide the names of people and places (CYCOM; Cohen).

At around 500 BC, The Spartans used a cryptographic device known as scytale which used a long strip of paper wound around a cylindrical staff to write down the message. After the message have been written, the paper is then unwrapped from the staff, thereby rearranging the characters, and would have to be rewrapped in a staff of similar diameter from the one that was used to write in order to read the message. The method used in this is called a transposition cypher. (CYCOM; Cohen; Calabrese 182-183)

Another method developed by the Greeks is the Polybius Square which lays down the alphabet in a five-by-five square. The rows and columns were numbered 1 to 5 so that each letter has a corresponding (row, column) pair. (CYCOM; Cohen)

At 50 BC, Julius Caesar uses a method of shifting the characters of the alphabet to obtain a cyphertext. This method is called a shift cypher, now known as the Caesar Cypher, which is one of the most famous substitution cyphers. It can be generally stated as substituting each plain letter with the

letter that is x places later in the alphabet, where x is between 1 to 25, and would be the key to the cypher. (CYCOM; Cohen; Calabrese 183; Singh 10)

The Caesar Cypher is an example of monoalphabetic cypher in which one character of a plaintext is substituted with a corresponding character in the cyphertext. Monoalphabetic cyphers are the easiest to break, or crack. In case of the Caesar Cypher, the codebreaker would only have to identify the correct key, which, in this case would only have 25 possibilities, to crack the message. Checking all the possible keys to crack a message is called the brute force method. The encryption of Caesar cypher in the English alphabet could be mathematically represented as $E_n(x) = (x + n) \bmod 26$; where x is the numerical equivalent of the letter (A= 1, B= 2,...) and n is is the key shift. Likewise, the decryption could be represented as $D_n(x) = (x – n) \bmod 26$.

A stronger version of a monoalphabetic cypher is a general substitution cypher, in which the cyphertext is derived from any rearrangement of characters in the alphabet of the plaintext. Considering there are 26 characters in a plaintext alphabet, there would be roughly 26! or 403, 291, 461, 126, 605, 635, 584, 000, 000 possible keys. However, a large number of keys is not the sole requirement for a secure cypher. It just makes the codebreaker’s job harder because a brute force method would be impractical (Singh 10).

One method of cracking a general monoalphabetic substitution cypher is to guess the meaning of a part of the cyphertext, which is called a crib (Singh 11). A cyphertext that appears to be in a letter format that starts in a

random four characters, say XBJA, could be assumed by a codebreaker to be the word ‘ dear’, which would mean that the true value of the cyphertext characters may, in fact be established and would be helpful in breaking the message. Without establishing a crib, however, a general substitution cypher is, indeed, very difficult to crack.

A 9 th century Arab philisopher named al-Kindi was the first to expose the weakness of general monoalphabetic substitution cyphers. His technique, now known as the frequency analysis, takes advantage of the fact that characters in the alphabet have a distinct variation in frequency. In English for example, ‘ e’ is the most commonly used letter, followed by the letters ‘ t’, ‘ r’, ‘ n’, ‘ i’, ‘ o’, and ‘ a’, while the letters ‘ x’, ‘ q’, and ‘ z’ are the rarest. Al-Kindi realized that if a letter (plaintext) was substituted for another letter (cyphertext), then the new letter (cyphertext) would have the same frequency as the original letter (plaintext). By studying the frequency of letters appearing in a cyphertext, it should be possible to establish their true value. (Singh 11; Bishop 7; Cohen)

In 1466, Leon Battista Alberti started the development of the polyalphabetic cypher which uses different cyphertext characters to represent the same plaintext symbol. Polyalphabetic cyphers are diffucult to break because each character of the plaintext is represented by different characters of the cyphertext. The most famous of the polyalphabetic cypher is the use of Vigenere Square, from its developer Blaise de Vigenere, from which the rows are composed of all the 26 Caesar cyphers at increasing shifts (the first row being the plaintext alphabet). The Vigenere cypher involves using several

rows of the Vigenere Square to convert the plaintext into cyphertext. The cryptographer might encrypt the message by using a certain row to convert the first letter, another row to convert the second, another to convert the third, and so on. To communicate, the sender and receiver must agree on a system for switching between rows, achieved by a keyword. The keyword is used to determine the row to which a specific letter will be converted. To do this, the keyword is spelled out above the message in a letter-to-letter correspondence and repeated over such that every letter in the plaintext has a corresponding letter from the keyword. Letters in the plaintext are encrypted using the row that starts with its corresponding keyword letter. (Singh 13)

The encryption of Vigenere cypher in English alphabet could mathematically be represented as $C_i = (P_i + K_i) \bmod 26$; where P is the numerical equivalent of the alphabet in the plaintext and K is the numerical equivalent of the keyword letter that corresponds to the plaintext letter. Likewise, the decryption could be represented as $P_i = (C_i – K_i) \bmod 26$.

In 1844, the development of cryptography was dramatically altered by the invention of the telegraph. In military, a base commander could be in instant communication with a field commander during battle and cyphers were needed to transmit information through telegraph. The Vigenere cypher was widely used at the time. The public also grew interest in cryptography an many individuals attmpted to formulate their own cypher systems. (Cohen)

The critical weakness of in the Vigenere cypher is the relatively short and repetitive nature of its key. If the key’s length could be determined then the

cyphertext could be treated as a series of different Caesar cyphers and could be broken by using frequency analysis. In 1863, Friedrich Wilhelm Kasiski published a successful attack on the Vigenere cypher, from which he argues that certain common words will, by chance, be encrypted using the same key letters leading to repeated groups in the cyphertext (Cohen). Taking advantage of this fact, a codebreaker can determine the length of the keyword and break the message. A new cypher was needed.

Tension of war in Europe was growing and cryptography was used widely even before the first world war broke. The English Black Chamber had been involved in solving cyphers for the government (Cohen).

In 1917, the British intercepted a coded telegram from Germany offering Mexico material aid and reclamation of territory lost during the Mexican-American War. The Americans shortly joined the British against the Germans in World War 1. Both sides employed cypher systems for tactical communications. In the same year, Gilbert Vernam of AT&T promoted the theory of one-time pad, which would make use of two identical pads printed with line of randomly generated numbers. The random numbers were used as shift values. Each sheet in the pad was different from the other and was only used once. Vernam also developed a machine to encrypt messages but was never widely used. (Calabrese 188; Bishop 18; CYCOM)

A series of cypher machines gained popularity with the onset of Industrial Revolution with the battle between cryptologists and codebreakers. Cypher machines usually use a Vigenere-like cypher but uses a general substitution cypher and not in a shift sypher. William Friedman began in 1917 the

process of applying statistical methods of cracking cyphers even those that were generated by cypher machines. This statistical method uses the Index of Coincidence—that is the number of times that identical letters appear in the same position. The Index of Coincidence can be mathematically represented as:

$$IC = \frac{\sum_{i=1}^{c} n_i (n_i - 1)}{N(N-1)/c}$$

where N is the length of the text, n_is are the frequencies of the ith letter of the alphabet. Computing the highest Index of Coincidence for every key length possible would determine the actual key length.

In 1927, the Enigma Machine was invented by a German named Arthur Scherbius. It generates a polyalphabetic cypher that uses an effectively unrepeating key, removing the weakness of the Vigenere cypher. The Germans believed the Enigma cypher was unbreakable, but British codebreakers at Bletchley Park, building on the work of their Polish allies, cracked the Enigma cypher. Cracking Enigma cyphers gave the allied forces advance knowledge of bombing raids. The radar, however, received much of the credits for the preparation of the defenders for incoming bombing raids. (Cohen; Calabrese 190; Singh 16)

Some of the first uses of computers were for decoding Enigma cyphers intercepted from the Germans (Cohen). With the changing technology and

tension in war is slowly decreasing, people had found other ways of using cryptography.

During the latter part of the 20 th century and into the new millenium, the growth and power of computing platforms and the crytographic needs of commercial business drives cryptography into a new era. Technological advances in computing minimizes the time required to conduct a brute force examination of character based cyphers. This trivializes the character cryptography problem space and requires cryptographic methods to increase complexity in order to be of any practical use. The development of information theory in 1949 by Claude Shannon was the basis of modern cryptography. Shannon determined for the first time a mathematically rigorous basis for defining a “ perfect” encryption system that could be made impenetrable, even in principle, to an adversary with unlimited resources. This forstered the growth of bit-wise mathematical cryptographic algorithms. By 1975, the National Bureau of Standards (now the National Institute of Standards and Technnology) promulgated the Data Encryption Standard (DES). (Dam 364-365; Calabrese 197)

Perhaps the most important result of Shannon’s contribution is the development of a measure of cryptographic strenght called the unicity distance, which indicates the number of cyphertext required to determine the message’s plaintext—that is, the length of the key used to encrypt the message and the statistical nature of the plaintext. Given enough time, it is guaranteed that any cypher can be broken given a length of cyphertext but also introduces the concept of workload, which embodies the difficulty in

determining the plaintext from cyphertext given the avilability of cyphertext to theoretically break the system. (Cohen)

Modern cryptography uses complex algorithms to convert plaintext into cyphetext. DES uses a fixed-length string of plaintext bits and transforms it through a series of operations into cyphertext bit string of the same length. Modern cryptography can help ensure the integrity of data—that is the data retrieved or received are identical to the original data stored or sent; to authenticate specific parties—that is to ensure that the purported sender is indeed the real sender; to facilitate nonrepudiation; and to preserve the confidentiality of information that may have come improperly into the possession of unauthorized parties (Dam 365).

Works Cited

Bishop, David. Introduction to Cryptography with Java Applets. Jones & Bartlett Publishers, 2002.

Calabrese, Tom and Thomas Calabrese. *Information Security Intelligence: Cryptographic Intelligence and Principles* . Thomson Delmar Learning, 2003.

Cohen, Fred. “ A Short History of Cryptography.” 1995. Fred Cohen and Associates. April 11, 2008.

Dam, Kenneth W. *Cryptography’s Role in Securing the Information Society* . National Academies Press, 1996.

Singh, Simon. “ A Brief History of Cyprography from Caesar to Bletchley Park.” *Colossus: The Secret of Bletchley Park’s Codebreaking Computers* . Oxford University Press, 2006.

“ A Brief History of Cryptography.” January 24, 2006. Cypher Research Laboratories Pty. Ltd (CYCOM). April 11, 2008. < http://www. cypher. com. au/crypto_history. htm >