Cryptography

I. What is Cryptography?

Do you have a message which is so confidential that you need to send to a certain person but you're afraid that somebody might read it? Well you better study about CRYPTOGRAPHY. But first what is cryptography? Cryptography is the study of hiding readable messages (plaintext) into a non-readable form (ciphertext). Based on my other source Cryptography is the practice and study of techniques for secure communication in the presence of third parties. To make it simple, Cryptography is used in order to make sure that your messages and data are secured from other elements.

The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext will result to meaningless data called ciphertext. We use encryption in order to hide the information from anyone whom is not intended even if they can see the encrypted data. But maybe you are curious on how your receiver will be able to read the unreadable message? Well if there is encryption, there is also decryption which is the reverse, in other words, moving from ciphertext back to plaintext. But in order to decipher a ciphertext, you should know the key used by the sender. A key is a usually a short string of characters, which is needed to decrypt a certain ciphertext.

Figure 1. 1 Encryption and decryption

Cryptography can be strong or weak. Cryptographic strength can be measured in the time it takes for one to recover the plaintext. The result of strong cryptography is a ciphertext that is very difficult to decipher without possession of the proper decoding tools.

According from another source, Cryptography is where security engineering meets mathematics. It provides us with tools that underlie most modern security protocols. It is widely used in the modern era to protect distributed systems from the wrong thing, or used to protect them in the wrong way.

Cryptography based on my other references is the study of methods to send and receive secret messages. The goal of cryptography to help a sender communicate a message to a receiver without the adversary learning what the message was. We know that there are tons of hackers who would want infiltrate a system and get information. Some will use that information in evil ways, some will sell it to companies and some just do it for fun. That's why cryptography is very essential to be learned and used especially when you are in the industry of modern technology.

Cryptography is also said to be the science and art of secret writing. It can protect data from unauthorized and unwanted disclosure; it can also authenticate the identity of a user of a program. So why do you think we should study cryptography? Well it is important for us to study cryptography since we are future programmers and future IT professionals because this would help us a lot especially in securing our programs. It will help us to ensure that the programs that we develop are safe from the hackers around us. It will also help us keep our job, imagine that you are responsible for the security of a system and it is infiltrated by hackers, definitely you will lose your job. Therefore as future programmers we should study and use cryptography wisely because this is very powerful but also dangerous in the hands of the wrong.

Figure1. 2 Key

II. History of Cryptography

No one really knows where or when cryptography started, some believe that it started when more than 3 individuals started to communicate, and when 1 of them wanted to send a message to another without being discovered by the others.

Classical Cryptography

Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4, 000 years. Cryptography probably began in or around 2000 B. C. in Egypt, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life. They are made cryptic, but its purpose is not to hide the text. Rather they are made in order to make it important to them. But as time pass by, the writing became more and more complicated, so the people lost interest to decipher them and soon the practice died out.

Cryptology was believed to be mysterious and enigmatic to most people back then. It was because of this that public began to believe that cryptography is related with black arts. They believed that it is used to communicate with dark spirits and unknown creatures. Most early cryptographers were scientists, but common people believed that they were also follower of the devil.

The ancient Chinese used the ideographic nature of their language to hide the meaning of the words. Messages were often transformed into ideographs for privacy, but no substantial uses in early Chinese military conquests are apparent.

In India, secret writing was apparently more advanced, and the government used secret codes to communicate with a network of spies spread throughout the country. Early Indian ciphers consisted mostly of simple alphabetic substitutions often based on phonetics. Some of these were spoken or used as sign language. This is somewhat similar to " pig latin" (igpay atinlay) where the first consenant is placed at the end of the word and followed by the sound " ay".

The cryptographic history of Messopotamia was similar to that of Egypt, in that cuneiforms were used to encipher text. This technique was also used in Babylon and Asyria. In the Bible, a Hebrew ciphering method is used at times. In this method, the last letter of the alphabet is replaced by the first, and vice versa. This is called 'atbash'. In the famous Greek drama the 'Iliad', cryptography was used when Bellerophon was sent to the king with a secret tablet which told the king to have him put to death. The king tried to kill him by having him fight several mythical creatures, but he won every battle. The Spartans used a system which consisted of a thin sheet of papyrus wrapped around a staff (now called a " staff cipher").

Messages were written down the length of the staff, and the papyrus was unwrapped. In order to read the message, the papyrus had to be wrapped around a staff of equal diameter. Called the 'skytale' cipher, this was used in the 5th century B. C. to send secret messages between greek warriors. Without the right staff, it would be difficult to decode the message using the techniques available at that time. Cryptanalysis is the practice of changing ciphertext into plaintext without complete knowledge of the cipher. The Arabs were the first to make significant advances in cryptanalysis.

An Arabic author, Qalqashandi, wrote down a technique for solving ciphers which is still used today. The technique is to write down all the ciphertext letters and count the frequency of each symbol. Using the average frequency of each letter of the language, the plaintext can be written out. This technique is powerful enough to cryptanalyze ANY monoalphabetic substitution cipher if enough cyphertext is provided. During the Middle Ages, cryptography started to progress. All of the Western European governments used cryptography in one form or another, and codes started to become more popular. Ciphers were commonly used to keep in touch with ambassadors. The first major advances in cryptography were made in Italy. Venice created an elaborate organization in 1452 with the sole purpose of dealing with cryptography.

World War II Cryptography

Cryptography is believed to be very important in war because a single message intercepted from the enemy can change the outcome of the battle. That’s why during the World War II, they already developed and used mechanical and electromechanical cipher machines, but these machines were impractical so manual systems are continued to be used. Great advancement occurred in both cipher design and cryptanalysis but all in secrecy. Information about this period has begun to be declassified as the official British 50-year secrecy period has come to an end, as US archives have slowly opened, and as assorted memoirs and articles have been published.

The Germans made heavy use of an electromechanical rotor based cipher system known as Enigma. The German military also developed several mechanical attempts at a one-time pad. Bletchley Park called them the Fish ciphers, and Max Newman and colleagues designed and deployed the world’s first programmable digital electronic computer, the Colosus, to help with their cryptanalysis. The German Foreign Office began to use the one-time pad in 1919; some of this traffic was read in World War II partly as the result of recovery of some key material in South America that was insufficiently carefully discarded by a German courier.

The Japanese Foreign Office used a locally developed electrical stepping switch based system, called Purple by the US, and also used several similar machines for attaches in some Japanese embassies. One of these called the ‘ M-machines’ by the US, another was referred to as ‘ Red’. All were broken to, one degree or another by the Allies.

Other cipher machines used in World War II included the British Typex and the American SIGABA; both were electromechanical rotor designs similar in spirit to the Enigma.

Figure 2. 1 Enigma Machine

Modern Cryptography

Beginning around the 1990s, the use of the Internet for commercial purposes and the introduction of e-commerce called for a widespread standard for encryption. Before the introduction of the Advanced Encryption Standard (AES), information sent over the Internet, such as financial data, was encrypted using the Data Encryption Standard (DES), a symmetric-key cipher. This was used for its speed, as DES could scramble massive amounts of data at high speeds. The problem with this was that over time, more users knew the key, and the risk of security breaches increased. Around the late 1990s to early 2000s, the use of the public-key became a more common approach for encryption, and soon a hybrid of the two schemes (key-wrapping) became the way for e-commerce operations to proceed. Additionally, the creation of a new protocol known as the Secure Socket Layer, or SSL, led the way for online transactions to take place. Transactions ranging from purchasing goods to online bill pay and banking used SSL. Furthermore, as wireless Internet connections became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations.

Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article entitled " A mathematical theory of cryptography". This article was written in 1945 and eventually was published in the Bell System Technical Journal in 1949. Shannon continued his work by producing another article entitled " A mathematical theory of communication". Shannon was inspired during the war to address "[t]he problems of cryptography [because] secrecy systems furnish an interesting application of communication theory". It is commonly accepted that this paper, published in 1949, was the starting point for development of modern cryptography. Shannon provided the two main goals of cryptography: secrecy and authenticity. His focus was on exploring secrecy and thirty-five years later, G. J. Simmons would address the issue of authenticity. " A mathematical theory of communication" highlights one of the most significant aspects of Shannon's work: cryptography's transition from art to science.

III. Three Types of Cryptography

There are many ways to classify cryptographic algorithms, but here we will categorize them depending on the number of keys that are used in encryption and decryption, and further defined by their application and use.

Figure 3. 1 Three Types of Cryptography

Secret Key Cryptography

In Secret Key Cryptography, only one key is used in both encryption and decryption. As shown in Figure 3. 1, the sender used a key to decrypt a plaintext and sends the ciphertext to the receiver. The receiver also used the same key in order to recover the plaintext. Secret Key Cryptography is also often called ' Symmetric Encryption' because only one key is used in both functions. It is obvious that in this kind of cryptography, both sender and receiver must know the key. The only problem is how the key is distributed.

Public Key Cryptography

The problem in key distribution was solved by Public key Cryptography which was introduced by Whitfield Diffie and Martin Hellman in 1975. Public key uses a pair of keys for encryption: a public key, which is used to encrypt a data, and a corresponding private, or secret key for decryption. You can publish your public key to the world but make sure to keep your private key. The purpose of this is for anyone also knows your public key, be able to encrypt data but they can never decrypt it unless they have the secret key.

The benefit of public key cryptography is that it allows people who have no preexisting security arrangement be able to communicate securely. The only problem is that secure channels and key distribution is very expensive so some are not able to use public key cryptography much.

Hash Function

The system mentioned above is said to have some problems. It is slow and it produces massive volume of data, at least double the size of the original information. An improvement on the above scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable-length Input in this case, a message of any length, even thousands or millions of bits and produces a fixed length output; say, 160-bits. The hash function ensures that, if the information is changed in any way even by just one bit an entirely different output value is produced.

IV. Morse code

Morse code is a method of transmitting text information as a series of on-off tones, lights, or clicks that can be directly understood by a skilled listener or observer without special equipment. It is also a method of sending messages by means of electronic pulses, which is usually represented as a short pulse, called a dot, and a long pause called dash. This code was developed by Samuel F. B Morse in the 1840s to work with his invention of the telegraph. There are various stories concerning how the Morse code was originally developed. According to one account, Samuel Morse went to a printer's shop and counted the amount of printer type the printer had for each letter of the alphabet. He then interpreted these counts as approximations of the relative frequency of each letter in typical English text. He organized the Morse code so that the shortest symbols were associated with the most frequent characters.

Thus, for example, E and T, the most often-used letters in the English language, were represented by a single dot and single dash, respectively. The least frequently occurring letters, such as J and Y, and numerals and punctuation marks were given longer and more complex representations. No differentiation was made for uppercase and lowercase. Each character (letters and numbers) were represented by unique sequence of dots and dashes. The duration of a dash is three times longer the duration of a Figure 4. 1 Chart of Morse Code dot. Each dot and dash is followed by a short silence, equal to the dot duration. The letters of a word are separated by a space equal to three dots (one dash), and two words are separated by a space equal to seven dots. The duration of the dot is considered as the basic unit of time measurement in code transmission.

Morse code speed is measured in words per minute or characters per minute. Operators who are skilled in Morse code can often understand code in their head at rates in excess of 40 wpm. Morse code is very useful because compared to voice, it is less sensitive to poor signal conditions, yet it is still comprehensible to human even without the help of decoding tools. In order to understand Morse code you need to memorize the value (dots and dash) of all the characters. It will not be that difficult because Morse code has its standard form. But you should be aware of your proper timing in order to understand the message being sent or vice-versa.

Morse code is an assistive technology, helping people with different disabilities to communicate. Morse can be sent by persons with severe motion disabilities, as long as they have some minimal motor control. Those people who are deaf or blind can also receive Morse through skin buzzer.

Morse code is composed of five elements, 1) Short mark, 2) Longer mark, 3) inter-element gap between the dots and dashes within a character, 4) short gap and 5) the medium gap. Morse code can be transmitted in various ways, from a tap of a finger to electrical pulses. Meaning Morse code is accessible to all. It can be used wherever you go as long as you have knowledge about it, making it very useful to communicate even without the use of other mechanical device. But sometimes problem occurs with the operator (sender) and the receiver because we all have different personal time, the operator may have shorter or longer pause than the receiver which will cause confusion between them. But all in all it is very helpful especially when it comes to radio, marines etc.