Chapter 1. Introduction to Cryptology

1.1. Introduction

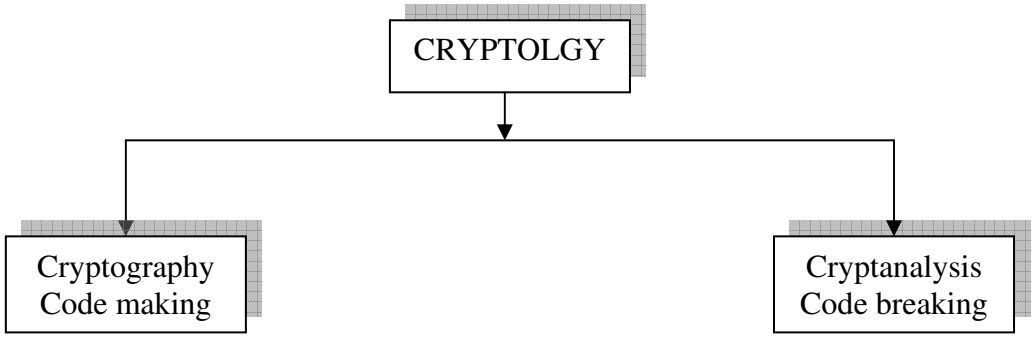
A brief overview of the development of secure communications methods from antiquity to the present day will be presented in this chapter. Keeping information hidden has been a large problem for humankind since its birth. So over the years man has come up with ways to alter (encrypt) their information so that others cannot tell what it says.

The science that studies secret communication is called cryptology. Secret writing has been employed as long as writing has existed; codes have been used throw history whenever people wanted to keep messages private. Cryptology has long been employed by governments, military, business and organizations to protect their messages.

The study of securing the content of messages is very old. Evidence suggests that it was used at least as early as the ancient Egyptians were. Diplomacy throughout the ages has relied upon the secrecy granted by cryptology, with some of history's great events being decided in major part by cryptography. Cryptology was very much a black art, obscure and limited, until the Second World War. The advent of radio, and the enormous distances involved, made cryptography necessary, and promoted the study of cryptanalysis. By far the most famous carpological story is the story of the cracking of the Germans Enigma code by the allies, and the corresponding advantages for them.

In this chapter, a briefly look at the history of cryptology will be done, and as these proceeds introducing various methods of obscuring message content, and looking at the ways in which these methods can be undone.

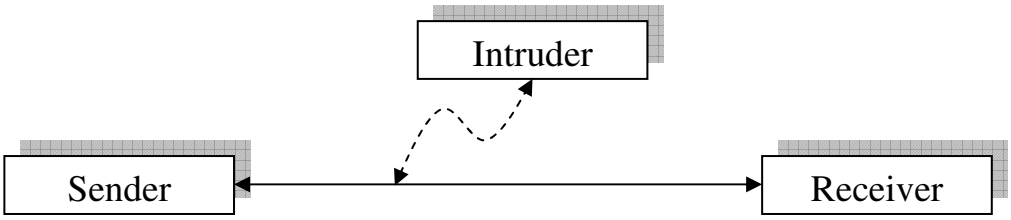
By this, some idea of the methods of cryptology will be given so the interesting properties of cryptology can be discussed intelligibly as a discipline. Cryptology: is the study of Cryptography (code making) and Cryptanalysis (code breaking). The use of Cryptography means can protect the information against various risks and attacks. [2, 3, 4, 55]



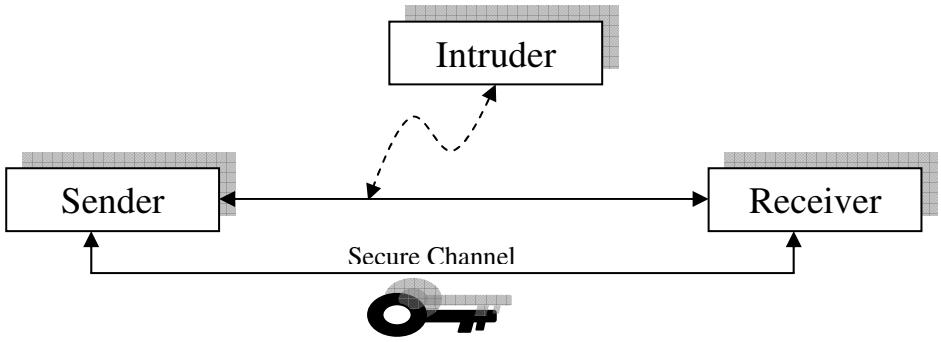
Figuer 1. Cryptology

1.2. Cryptography

The word cryptography comes from Greek words Kryptos, meaning hidden, and Graphen, meaning to write. Cryptography is the science and art of secret writing - keeping information secret when applied in computing environment, Cryptography can protect data against unauthorized disclosure as shown in the two following figures according to Shannon. [2, 3]



Figuer 2. Shannon Model



Figuer 3. Shannon Model with a key

Cryptography was once the science and art of diplomatic and military communication to prevent disclosure of the contents of the messages between diplomatic positions and army units. With modern telecommunication this methods were used even more heavily than at the beginning of its history. History of cryptology is as old as history of diplomacy and warfare. Use of cryptography has spread to civilian areas. Whenever you use mobile telephone, you use a radio transmitter where the communication between the telecom transmitter and your handset is ciphered to prevent listening of other handsets. [5, 6]

1.3. A Brief History of Cryptography

Knowledge of cryptography can be traced back to ancient times, it is not difficult to understand why: as soon as three people had mastered the art of reading and writing, there was the possibility that two of them would want to send letters to each other that the third could not read.

1.3.1. Ancient Egyptian

Researchers have dates as early as four thousand years ago for the first documented cases of encryption .It is said that the ancient Egyptian used encryption technique. It seems that encryption started with Egyptian partly by accident. Some ancient Egyptian writers often would substitute some hieroglyphs for a series of others. One reading the writing, if not aware of the substitutions, could not comprehend the writing. Noticing this some Egyptians started encrypting information on purpose. It is thought secret religious practices from those not involved. [2]

1.3.2. Ancient Greece

The Greeks, some time later developed a method called the transposition cipher where words are transposed for encryption. Transposition ciphers perform some sort of permutation on the plaintext letters. For example: (thequickbrownfox) becomes (foxthebrownquick). In Sparta, a province in Greece, the Spartans were known to have invented the (Skytale) where a

parchment is wrapped around a stick or staff so that when written upon and removed from the stick it was not easily read. [2]

The Greeks also provide one of the first literary references to cryptography .in (the ILLIAD) by homer, a messenger is sent to the king write a secret message telling the king with a secret message telling the king to kill him. Briefly, Scytale Cipher can be defined as follows:

- An early Greek transposition cipher
- A strip of paper was wound round a staff
- Message written along staff in rows, then paper removed
- Leaving a strip of seemingly random letters
- Not very secure as key was width of paper & staff

1.4. Classical Cryptographic Techniques

There are two basic components of classical ciphers: substitution and transposition

- In substitution ciphers letters are replaced by other letters, where in transposition ciphers letters are arranged in a different order
- These ciphers may be:
    - **Mono-alphabetic**: only one substitution/transposition is used, or
    - **Poly-alphabetic**: several substitutions/transpositions are used
- Several such ciphers may be come together to form a product cipher

1.4.1. Columnar transpositions:

A columnar transposition cipher is a simple hobbyist cipher in which the order of the letters in a message is changed, but the letters themselves are left unchanged.

The cipher is performed by writing the message into a grid, and then taking the letters out in a different order. The letters are written into the grid straight across the rows. Here, 'this is a sample' message had been written into a 5-column grid.