Cryptology is the science and study of systems for secret communications. It consists of two complementary fields of study: **Cryptography, and Cryptanalysis.**

Cryptography: It is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication**.**
Cryptography classified into two types: 1. Symmetric 2. Asymmetric

A Symmetric cryptography ciphers may in fact be sub classified into Block Ciphers (in which blocks of data, known as plaintext, are transformed into cipher textwhich appears unintelligible to unauthorized persons) and Stream Ciphers.

There are two types of network security:

1. **Symmetric key encryption** :it's a system when the sender encrypt the message with a specific key and the receiver use the same key to decrypt the encrypted message.
2. **Asymmetric key encryption** :it's a system when the sender encrypt the message with a specific key and the receiver use different key to decrypt the encrypted message.

There are five special ingredients in each encryption and decryption methods which are:

1. **Plaintext** :This is the original intelligible message or data that is fed into the algorithm as input.
2. **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
3. **Secret key:** The secret key is also input to the encryption algorithm .The key is a value independent of the plaintext and of the algorithm.
4. **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
5. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

A Symmetric cryptography ciphers may in fact be sub classified into:

1. **Block Cipher**: processes the input one block of elements at a time, producingan output block for each input block.
2. **Stream Cipher:** processes that encrypt a digital data stream one bit or onebyte at a time.

Cryptosystem: The package of all processes, formulae, and instructions for encoding and decoding messages using cryptography.

Substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns. There are a number of different types of substitution cipher:

1. **Monoalphabetic**: Using one alphabet - refers to a cryptosystem where each alphabetic character is mapped to a unique alphabetic character.

2. **Polyalphabetic**: Using many alphabets - refers to a cipher where each alphabetic character can be mapped to one of many possible alphabetic characters.

Transposition technique is a very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.

Cryptanalysis

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

The most common types of attack models are:

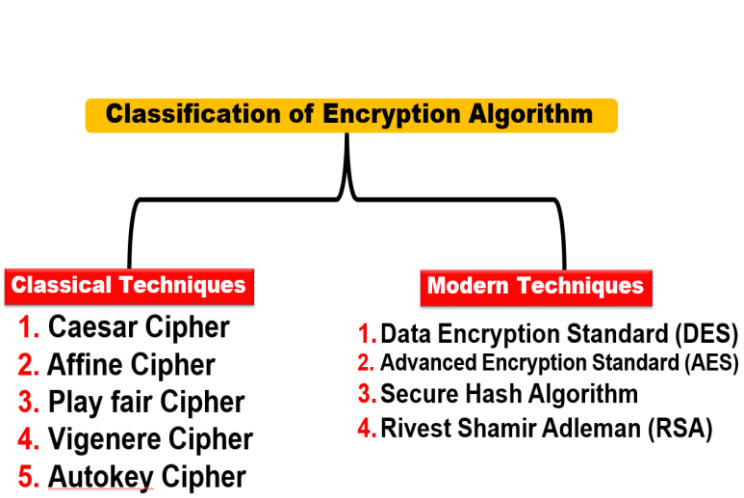
1. **Ciphertext only attack:** The opponent possesses a string of ciphertext, y.
2. **Known plaintext attack:** The opponent possesses a string of plaintext, x and the corresponding ciphertext, y.
3. **Chosen plaintext attack:** The opponent has obtained temporary access to the encryption machinery. Hence he can choose a plaintext and construct the corresponding ciphertext
4. **Chosen ciphertext attack:** The opponent has obtained temporary access to the decryption machinery. Hence he can choose a ciphertext, and construct the corresponding ciphertext.

Cryptanalysis of Caesar Cipher

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed. A brute-force attack involves systematically checking all possible keys until the correct key is found. Simply try all the 25 possible keys. In this case, the plaintext leaps out as occupying the third line. Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

There is, however, another line of attack. If the cryptanalyst knows the nature of the plaintext, then the analyst can exploit the regularities of the language. As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English. If the message were long enough, this technique alone might be sufficient, but because this is a relatively short message, we cannot expect an exact match. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.



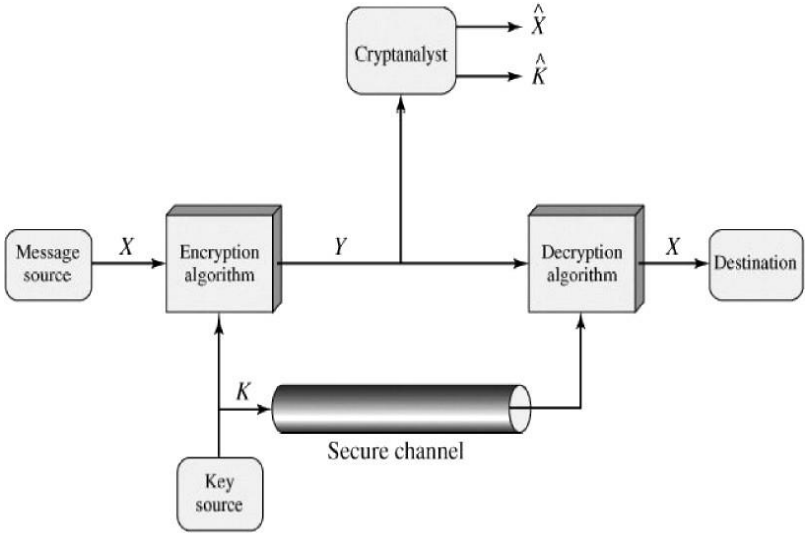


Figure 1-2: Model for Network Security

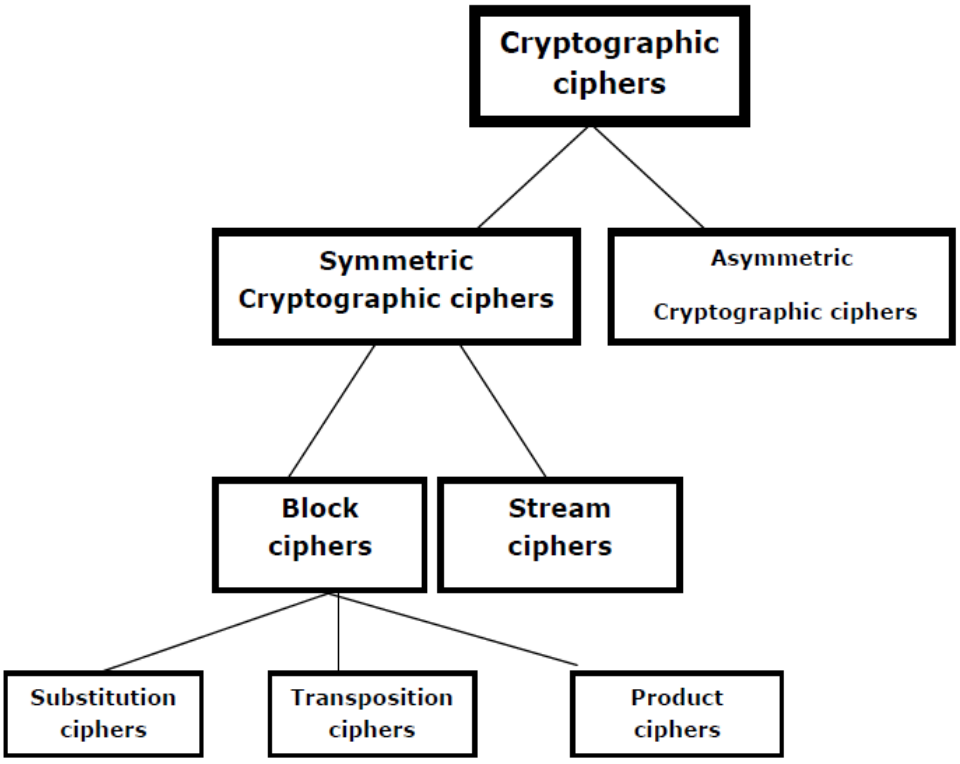


Figure1-1: Schematic representation of cryptographic cipher classification