Cryptography: is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security.

The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information.

By far the most important automated tool for network and communications security is encryption. Two forms of encryption are in common use: conventional, or symmetric encryption and public-key, or asymmetric, encryption.

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

Cryptology primarily has been applied in military and diplomatic communications systems, but other significant applications are becoming apparent.

Cryptography methods applied by authorized information sharers to design and develop encryption schemes in order to ensure confidentiality of information.

Crypt-Analysis (mathematical and statistical attempts by unauthorized persons to break cipher in order to reveal the meaning of the underlying protected data).

Cryptography:

It is the study of mathematical techniques related to aspects of information security such as: -

- **Confidentiality** is the concealment of information or resources.
- **Authenticity** is the identification and assurance of the origin of information.
- **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Availability** refers to the ability to use the information or resource desired.
- **Non-repudiation** It implies that one party of a transaction cannot deny having

received a transaction, nor can the other party deny having sent a transaction.

Classification of Cryptography

- Number of keys used
  - Hash functions: no key
  - Symmetric encryption (Private Key): one key
  - Asymmetric encryption (Public Key): two keys - public, private
- Type of encryption operations used
  - substitution / transposition / product
- Way in which plaintext is processed
  - block / stream

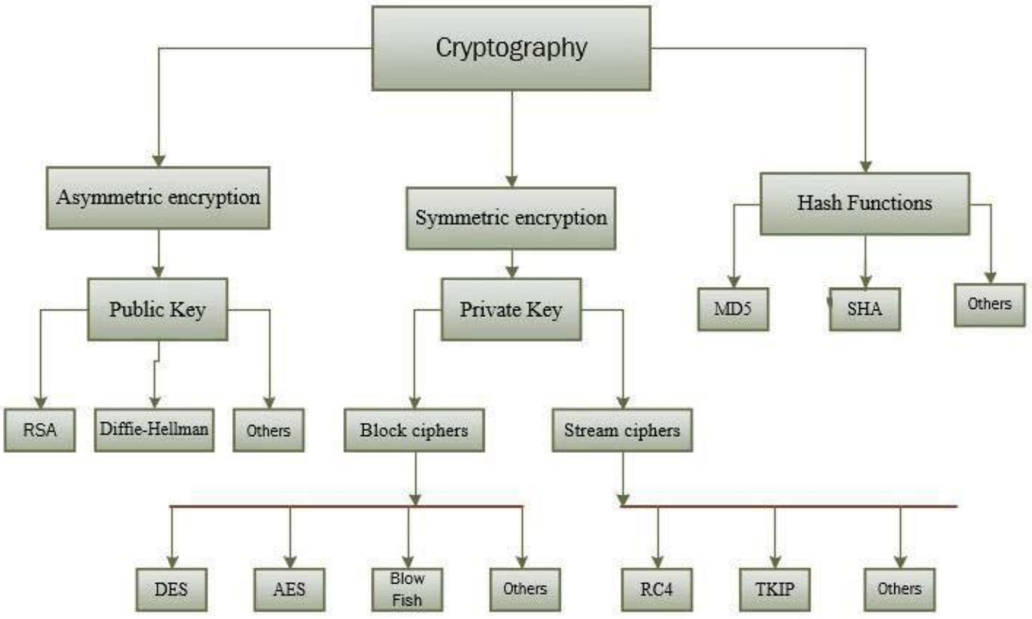

Figure 1-1 Schematic representation of cryptographic cipher classification

Symmetric Ciphers

In Symmetric cryptography ciphers the enciphering and deciphering keys are the same, as shown in figure 1-2:

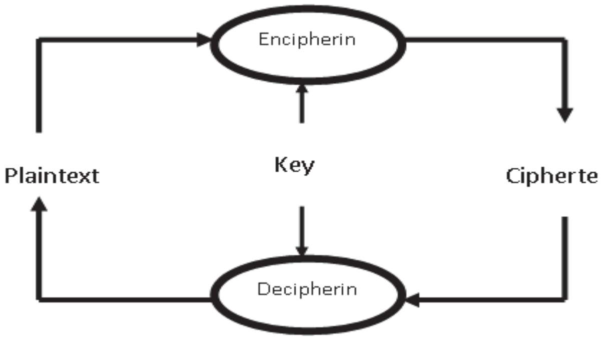

Fig. 1-2: Secret Writing

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

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

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

The process of transforming plaintext into ciphertext is called **<u>Encryption</u>**; the reverse process of transforming ciphertext into plaintext is called **<u>Decryption</u>**.

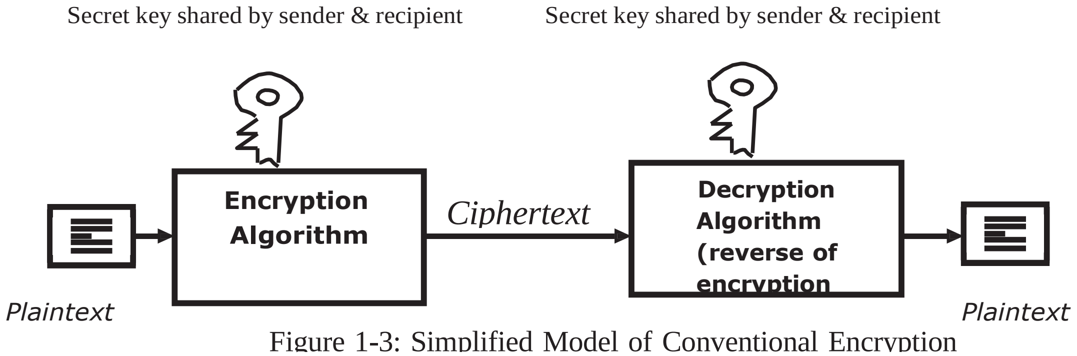
Secret key shared by sender & recipient
Secret key shared by sender & recipient
Encryption Algorithm
Ciphertext
Decryption Algorithm (reverse of encryption
Plaintext
Plaintext

Figure 1-3: Simplified Model of Conventional Encryption

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Note: Enciphering

Plaintext ➔ small letter

Key ➔ capital letter

Cipher text ➔ capital letter

Deciphering

Ciphertext➔ capital letter

Key ➔ small letter

Plain text➔ small letter

Block: A sequence of consecutive characters encoded at one time.

Block length: The number of characters in a block.

An algorithm for performing encryption (and the reverse, decryption): a series of well-defined steps that can be followed as a procedure. It works at the level of individual letters, or small groups of letters.

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

Digram: Sequence of two consecutive characters

Key: A relatively small amount of information that is used by an algorithm to customize the transformation of plaintext into ciphertext (during encryption) or vice versa (during decryption)

Key length: The size of the key - how many values comprise the key

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

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

Trigram: Sequence of three consecutive characters unigram

A model for much of what we will be discussing is captured, in very general terms, in figure 1-4. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

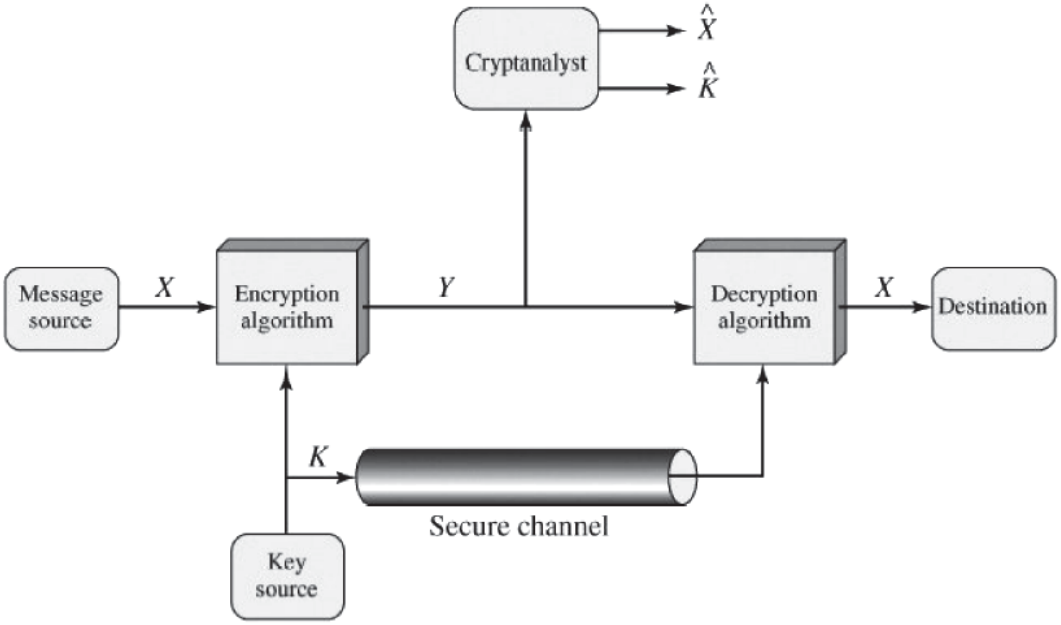

Figure 1-4: Model for Network Security

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender, some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Part Two discusses a form of encryption, known as public-key encryption, in which only one of the two principals needs to have the secret information.

Secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

However, there are other security-related situations of interest that do not neatly fit this model. A general model of these other situations is illustrated by Figure 1-5, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

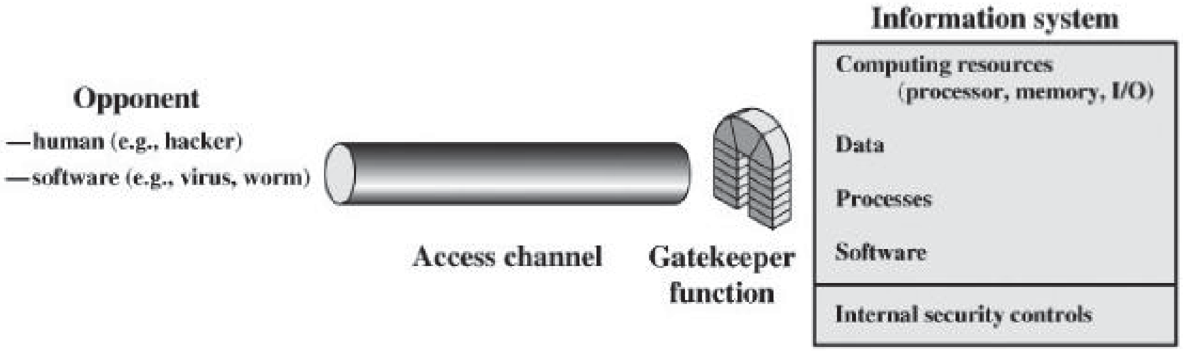

Figure 1-6: Network Access Security Model

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

Information access threats intercept or modify data on behalf of users who should not have access to that data.

Service threats exploit service flaws in computers to inhibit use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories:

1. The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access.
2. The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.