Date : 01/02/2021 Subject : Cryptography & System Security

Lecture No : 3

Topics Covered :
1. Security Services & Mechanisms
2. Network Security Model
3. Symmetric Cipher Model

Definition :

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

Perhaps a clearer definition is found in RFC 4949, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources

To Remember :

Security Services implement security policies and are implemented by security mechanisms.

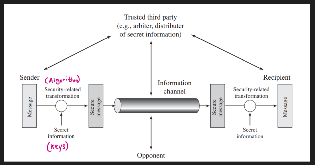
Security Services

1. Authentication
2. Access Control
3. Confidentiality
4. Integrity
5. Non Repudiation
6. Availability

Security Mechanisms

1. Encipherment
2. Digital Signature
3. Access Control
4. Data Integrity
5. Authentication Exchange
6. Traffic Padding
7. Routing Control
8. Notarization

Network Security Model



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.

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.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the 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.

Some Basic Definitions :

Before beginning, we define some terms.

1. An original message is known as the plaintext, while the coded message is called the ciphertext.

2. The process of converting from plaintext to ciphertext is known as enciphering or encryption;

3. restoring the plaintext from the ciphertext is deciphering or decryption.

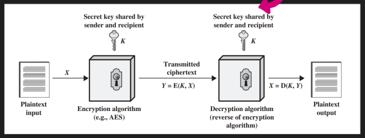
4. The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher.

5. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code."

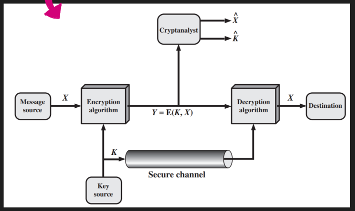
6. The areas of cryptography and cryptanalysis together are called cryptology.

Symmetric Cipher Model

Simplified Model of Symmetric Encryption



Practical Model of Symmetric Encryption



A symmetric encryption scheme has five components:

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

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

- 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. 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.

- Ciphertext:
This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

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