13.8.2.1. Message Security

Unit : 4 Network Security

Here, we shall discuss the security measures applied to each single message. The security provides four services as shown in figure 13.12.

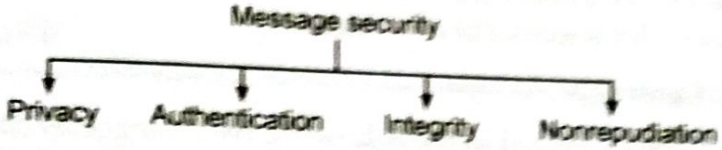

Fig. 13.12. Message security

(1) Privacy

The transmitted message must be such that only the intended receiver should be able to read it. No one else should be able to read it. The privacy is achieved by means of using the encryption. We can use the symmetric key encryption and decryption. It is also possible to use public key encryption to achieve the privacy.

(2) Message Authentication

In message authentication, the receiver needs to be sure about the sender's identity. Digital signature is used for providing the message authentication.

(3) Integrity

We can define the meaning of integrity as the data arriving at the receiver exactly, as it was sent. They should not be changed absolutely. The digital signature can provide message integrity.

(4) Nonrepudiation

The meaning of nonrepudiation is that the receiver should be able to prove that the message it has received has come from a specific sender. The digital signature can provide the nonrepudiation.

13.8.3. Performance Comparison of Secret Key and Public Key Cryptosystems

S.No.	Secret key system	Public key system
1.	It is also called as symmetrical key	It is also called as asymmetrical key system. system.
2.	Each sender and receiver pair has	The sender uses the public key while to use a unique key.receiver uses its own private key.
3.	It is more efficient.	It is less efficient.
4.	It is useful for encryption and decryption of long message.	It is used for encryption and decryption of short messages.
5.	A large number of keys are required.	The number of keys is less.

13.2. CRYPTOGRAPHY COMPONENTS UNIT 4: Network Security (Page-2)

Cryptography is Greek word which means *secret writing*. Figure 13.1 shows the cryptography components.

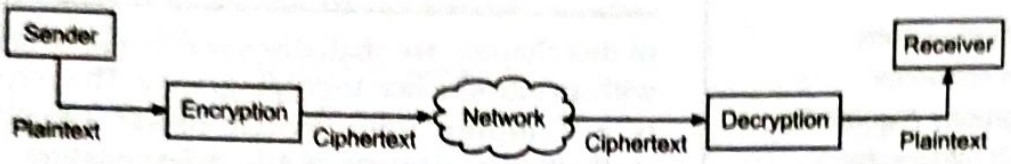

Fig. 13.1. Cryptography components

1. Plaintext

The original message produced by the sender is called as plaintext. It is data before transmission.

2. Ciphertext

The plaintext is transformed into ciphertext. The encryption program converts the plaintext into ciphertext.

3. Decryption

Decryption is a process which is exactly opposite to encryption. The decryption algorithm at the receiver transforms the ciphertext back to plaintext.

4. Ciphers

The encryption and decryption algorithms together are referred to as ciphers. This term is also used to refer to different categories of algorithms in cryptography. It is not necessary to have a separate cipher for each sender or receiver pair. Instead, it is possible to use public ciphers with secret keys for millions of pair of sender and receiver.

5. A Key

A key is a value or a number. The cipher as an algorithm operates on the key. For the encryption of a message, we have to use an encryption algorithm, an encryption key and the plaintext at the input as shown in the figure 13.2 (a). At the output of the encryption box, we get the ciphertext. For

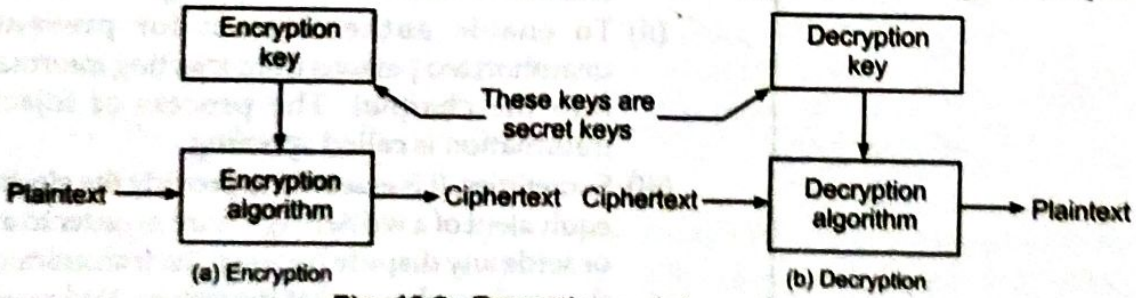

Fig. 13.2. Encryption and decryption