13.3. TYPES OF CRYPTOGRAPHY ALGORITHMS

UNIT 4: Network Security (Page-3

Basically, the cryptography algorithms may be classified into following two types as under:

(i) Symmetric key or secret key cryptography algorithms and

(ii) Public key or asymmetric cryptography algorithms.

Let us discuss them one by one.

13.4. SYMMETRIC KEY CRYPTOGRAPHY

1. Basic concepts

It is also called as the secret key cryptography. Figure 13.3 shows the block schematic of symmetric key cryptography.

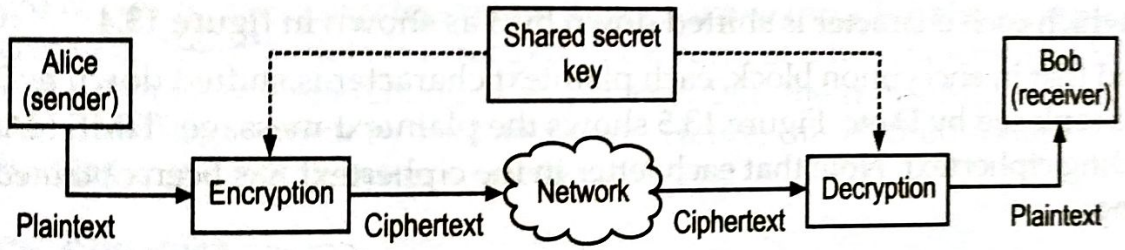

Fig. 13.3. Illustration of symmetric key cryptography

In the symmetrical key cryptography, the same key (shared secret key) is used by the sender and receiver.

The sender uses this key alongwith the encryption algorithm to encrypt the data, and the receiver uses it alongwith the decryption algorithm to decrypt the data. The encryption algorithm makes use of a combination of addition and multiplication whereas the decryption algorithm uses a combination of subtraction and division.

2. Advantages

(i) The major advantages of symmetric key algorithm is that it is more efficient than the public key algorithms. It takes less time to encrypt a message using the symmetric key algorithm. This is because this key is of smaller size (length)

(ii) Hence, symmetric key algorithms are used for encryption and decryption of long messages.

3. Drawbacks

(i) The first drawback is that the sender and receiver both should have a unique symmetric key. Therefore, a large number of keys are required when the numbers of users increases.

(ii) The distribution of keys between two users can be difficult.

1. Basic Concepts

The public key cryptography is also called as the asymmetric key cryptography. In this type of cryptography, there are two keys as under:

(i) Private key

(ii) Public key.

Out of them, the private key is kept by the receiver whereas the public key is announced to the public. Figure 13.10 shows the schematic for public key cryptography.

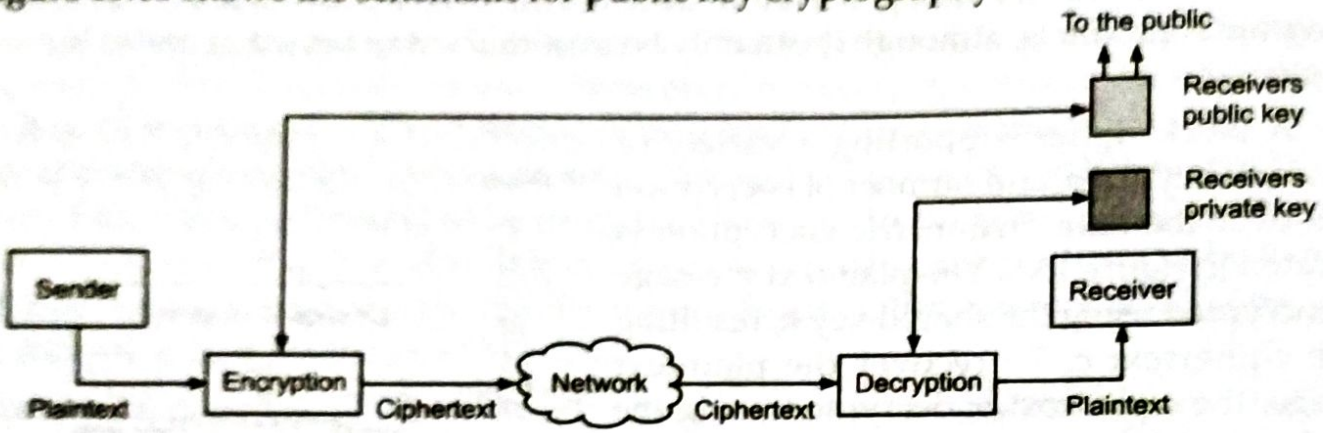

Fig. 13.10. Illustration of public key cryptography

In this system, the sender uses the public key to encrypt the message to sent. At the receiver, this message is decrypted with the help of receivers private key. The public key used for encryption is different from the private key used for decryption. The public key is known to everyone but the private key is available only to an individual

2. Advantages

(i) There is no compulsion of using (sharing) the symmetric key by the sender and receiver.

(ii) The number of keys required reduces tremendously.

3. Drawbacks

(i) The algorithms used are highly complex.

(ii) It takes a long time to calculate ciphertext from plaintext.

(iii) It is necessary to verify the association between a sender and this public key.