Module 8

Network Security

Lesson 1

Cryptography

Specific Instructional Objectives

On completion, the students will be able to:

- State the need for secured communication
- Explain the requirements for secured communication
- Explain the following cryptographic algorithms:
  - Symmetric-key Cryptography
    - Traditional ciphers
    - Monoalphabetic Substitution
    - Polyalphabetic Substitution
    - Transpositional Cipher
    - Block ciphers
  - Public-key Cryptography
    - The RSA Algorithm

8.1.1 Introduction

The word **cryptography** has come from a Greek word, which means *secret writing*. In the present day context it refers to the tools and techniques used to make messages secure for communication between the participants and make messages immune to attacks by hackers. For private communication through public network, cryptography plays a very crucial role. The role of cryptography can be illustrated with the help a simple model of cryptography as shown in Fig. 8.1.1. The message to be sent through an unreliable medium is known as **plaintext**, which is encrypted before sending over the medium. The encrypted message is known as **ciphertext**, which is received at the other end of the medium and decrypted to get back the original plaintext message. In this lesson we shall discuss various cryptography algorithms, which can be divided into two broad categorize - **Symmetric key cryptography** and **Public key cryptography.** Cryptography algorithms based on symmetric key cryptography are presented in Sec. 8.1.2. Public key cryptography has been addressed in Sec. 8.1.3.

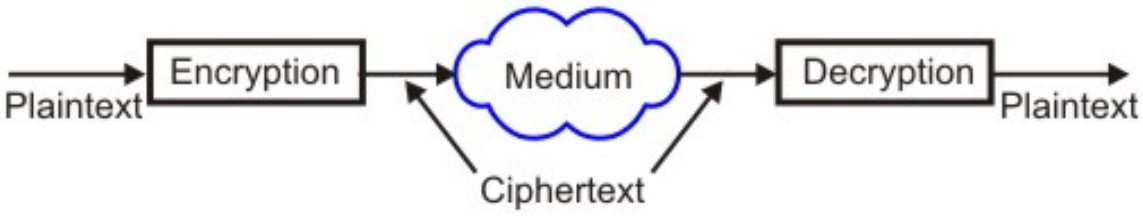

Figure 8.1.1. A simple cryptography model

8.1.2 Symmetric Key Cryptography

The cipher, an algorithm that is used for converting the plaintext to ciphertex, operates on a **key**, which is essentially a specially generated number (value). To decrypt a secret message (ciphertext) to get back the original message (plaintext), a decrypt algorithm uses a decrypt key. In symmetric key cryptography, same key is shared, i.e. the same key is used in both encryption and decryption as shown in Fig. 8.1.2. The algorithm used to decrypt is just the inverse of the algorithm used for encryption. For example, if addition and division is used for encryption, multiplication and subtraction are to be used for decryption.

Symmetric key cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages. However, these algorithms suffer from the following limitations:

- Requirement of large number of unique keys. For example for n users the number of keys required is n(n-1)/2.
- Distribution of keys among the users in a secured manner is difficult.

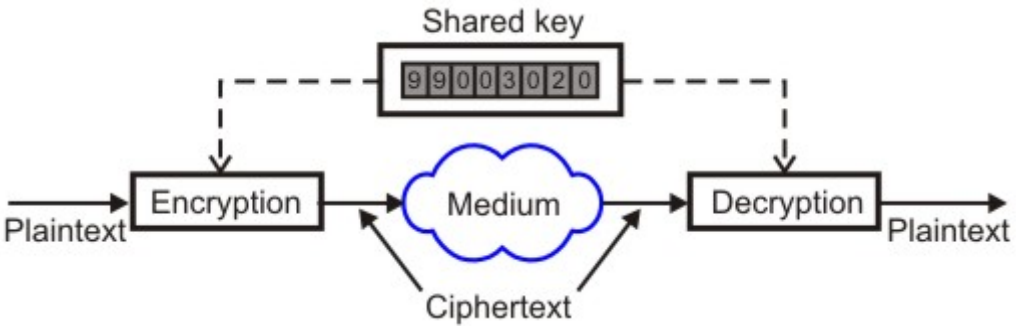

Figure 8.1.2. A simple symmetric key cryptography model

8.1.2.1 Monoalphabetic Substitution

One simple example of symmetric key cryptography is the *Monoalphabetic substitution*. In this case, the relationship between a character in the plaintext and a character in the ciphertext is always one-to-one. An example Monoalphabetic substitution is the Caesar cipher. As shown in Fig. 8.1.3, in this approach a character in the ciphertext is substituted by another character shifted by three places, e.g. A is substituted by D. Key feature of this approach is that it is very simple but the code can be attacked very easily.

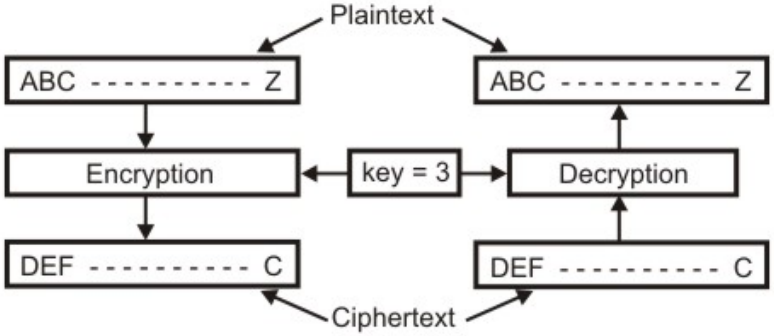

Figure 8.1.3. The Caesar cipher

8.1.2.2 Polyalphabetic Substitution

This is an improvement over the Caesar cipher. Here the relationship between a character in the plaintext and a character in the ciphertext is always one-to-many.

Example 8.1: Example of polyalphabetic substitution is the Vigenere cipher. In this case, a particular character is substituted by different characters in the ciphertext depending on its position in the plaintext. Figure 8.1.4 explains the polyalphabetic substitution. Here the top row shows different characters in the plaintext and the characters in different bottom rows show the characters by which a particular character is to be replaced depending upon its position in different rows from row-0 to row-25.

- Key feature of this approach is that it is more complex and the code is harder to attack successfully.

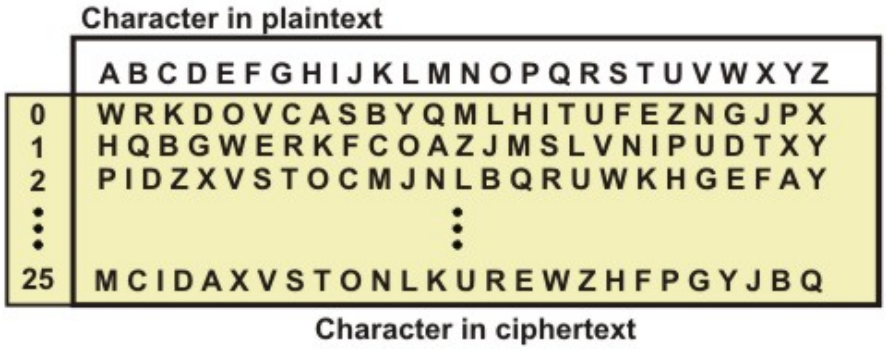

Figure 8.1.4. Polyalphabetric substitution

8.1.2.3 Transpositional Cipher

The transpositional cipher, the characters remain unchanged but their positions are changed to create the ciphertext. Figure 8.1.5 illustrates how five lines of a text get modified using transpositional cipher. The characters are arranged in two-dimensional matrix and columns are interchanged according to a key is shown in the middle portion of the diagram. The key defines which columns are to be swapped. As per the key shown in the figure, character of column is to be swapped to column 3, character of column 2 is to be swapped to column 6, and so on. Decryption can be done by swapping in the reverse order using the same key.

Transpositional cipher is also not a very secure approach. The attacker can find the plaintext by trial and error utilizing the idea of the frequency of occurrence of characters.

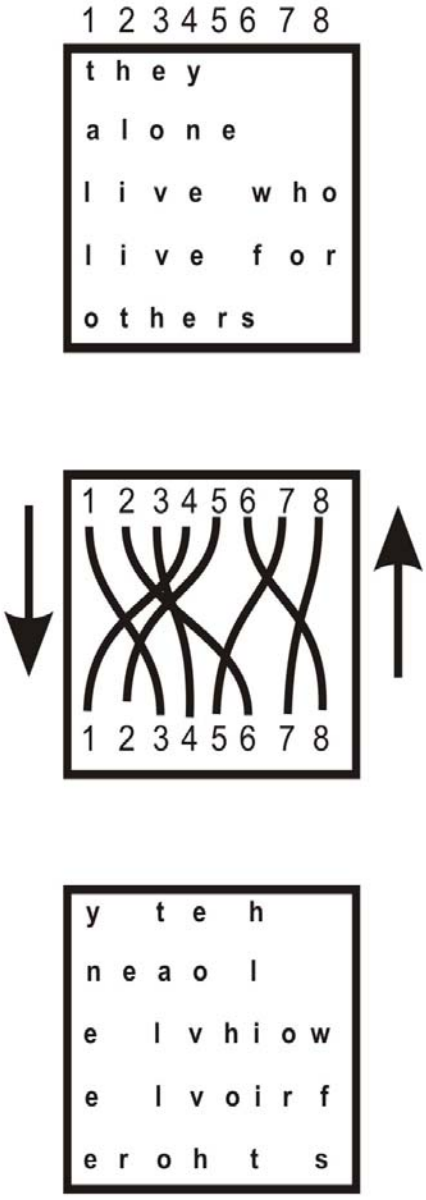

Figure 8.1.5. Operation of a transpositional cipher

8.1.2.4 Block Ciphers

Block ciphers use a block of bits as the unit of encryption and decryption. To encrypt a 64-bit block, one has to take each of the 2^{64} input values and map it to one of the 2^{64} output values. The mapping should be one-to-one. Encryption and decryption operations of a block cipher are shown in Fig. 8.1.6. Some operations, such as permutation and substitution, are performed on the block of bits based on a key (a secret number) to produce another block of bits. The permutation and substitution operations are shown in Figs 8.1.7 and 8.1.8, respectively. In the decryption process, operations are performed in the reverse order based on the same key to get back the original block of bits.

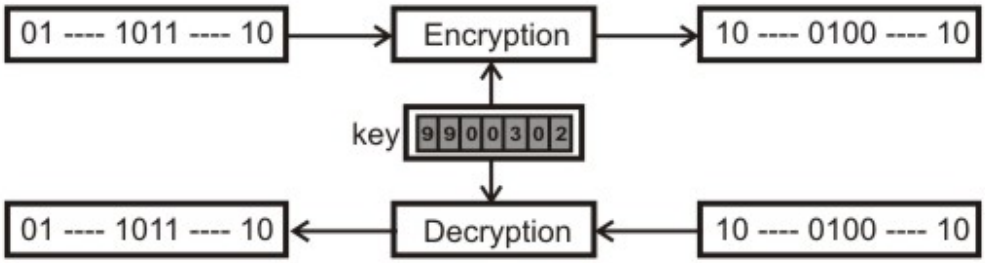

Figure 8.1.6. Transformations in Block Ciphers

Permutation: As shown in Fig. 8.1.7, the permutation is performed by a permutation box at the bit-level, which keeps the number of 0s and 1s same at the input and output. Although it can be implemented either by a hardware or a software, the hardware implementation is faster.

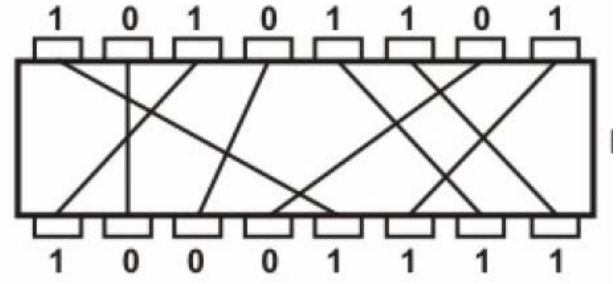

Figure 8.1.7. Permutation operation used in Block Ciphers

Substitution: As shown in Fig. 8.1.8, the substitution is implemented with the help of three building blocks – a decoder, one p-box and an encoder. For an n-bit input, the decoder produces an 2^n bit output having only one 1, which is applied to the P-box. The P-box permutes the output of the decoder and it is applied to the encoder. The encoder, in turn, produces an n-bit output. For example, if the input to the decoder is 011, the output of the decoder is 00001000. Let the permuted output is 01000000, the output of the encoder is 011.

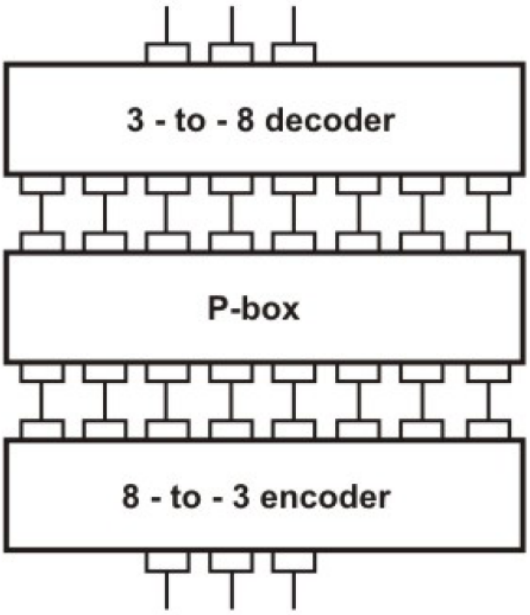

Figure 8.1.8. Substitution operation used in Block Ciphers

A block Cipher: A block cipher realized by using substitution and permutation operations is shown in Fig. 8.1.9. It performs the following steps:

Step-1: Divide input into 8-bit pieces
Step-2: Substitute each 8-bit based on functions derived from the key
Step-3: Permute the bits based on the key

All the above three steps are repeated for an optimal number of rounds.

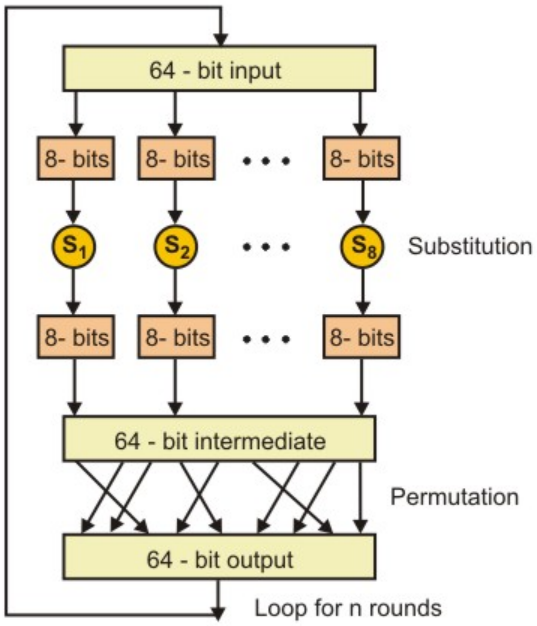

Figure 8.1.9.Encryption by using substitution and permutation

8.1.2.5 Data Encryption Standard (DES)

One example of the block cipher is the Data Encryption Standard (DES). Basic features of the DES algorithm are given below:

- A monoalphabetic substitution cipher using a 64-bit character
- It has 19 distinct stages
- Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length.
- The decryption can be done with the same password; the stages must then be carried out in reverse order.
- DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the ciphertext.
- As the number of rounds increases, the security of the algorithm increases exponentially.
- Once the key scheduling and plaintext preparation have been completed, the actual encryption or decryption is performed with the help of the main DES algorithm as shown in Fig. 8.1.10.

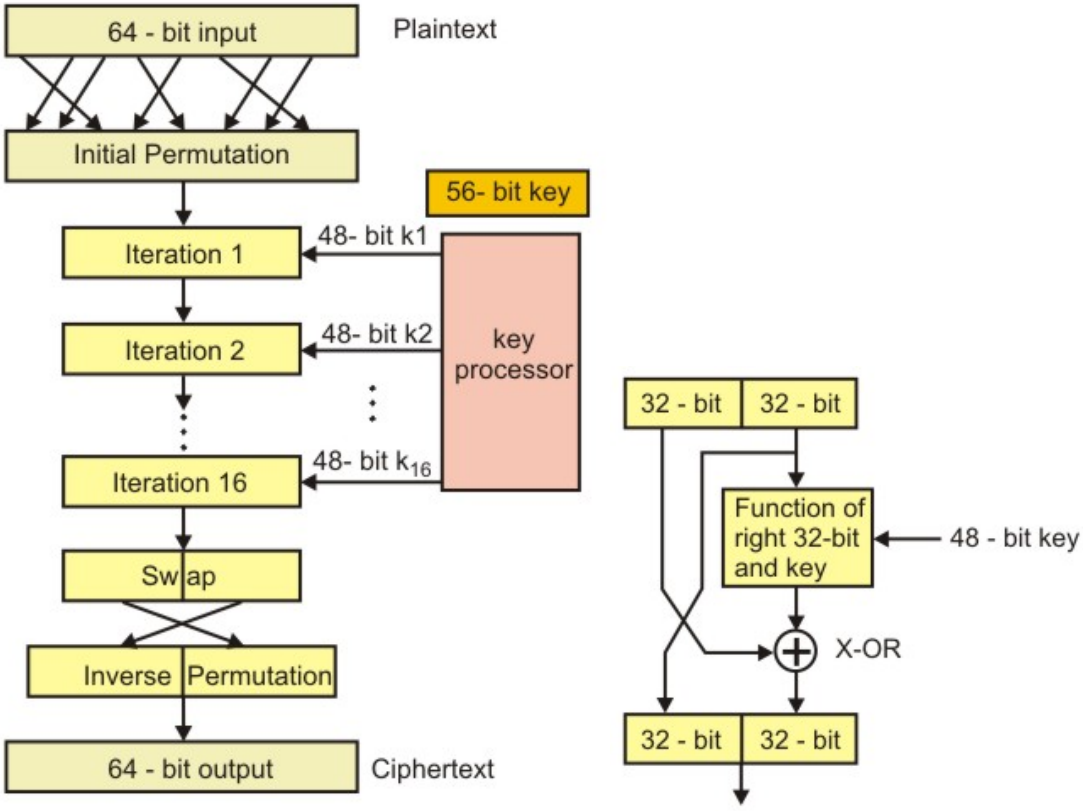

Figure 8.1.10 64-bit Data Encryption Standard (DES)

8.1.2.6 Encrypting a Large Message

DES can encrypt a block of 64 bits. However, to encrypt blocks of larger size, there exist several modes of operation as follows:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)

Electronic Code Book (ECB)

This is part of the regular DES algorithm. Data is divided into 64-bit blocks and each block is encrypted one at a time separately as shown in Fig. 8.1.11. Separate encryptions with different blocks are totally independent of each other.

Disadvantages of ECB

- If a message contains two identical blocks of 64-bits, the ciphertext corresponding to these blocks are identical. This may give some information to the eavesdropper
- Someone can modify or rearrange blocks to his own advantage
- Because of these flaws, ECB is rarely used

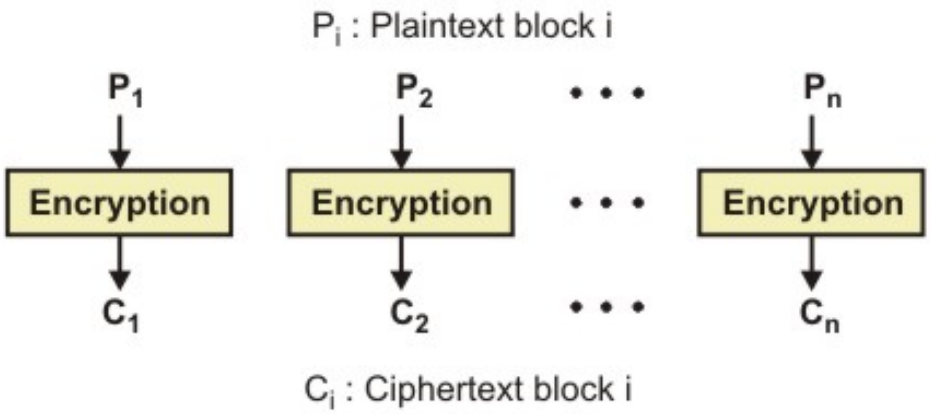

Figure 8.1.11 Electronic Code Book (ECB) encryption technique

Cipher Block Chaining (CBC)

In this mode of operation, encrypted ciphertext of each block of ECB is XORed with the next plaintext block to be encrypted, thus making all the blocks dependent on all the previous blocks. The initialization vector is sent along with data as shown in Fig. 8.1.12.

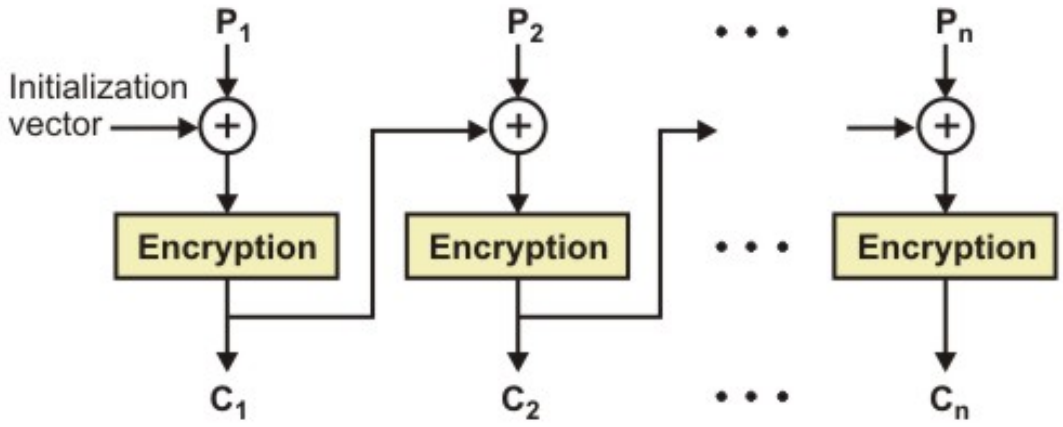

Figure 8.1.12 Cipher Block Chaining (CBC) encryption technique

Cipher Feedback Mode (CFB)

- In this mode, blocks of plaintext that is less than 64 bits long can be encrypted as shown in Fig. 8.1.13.
- This is commonly used with interactive terminals
- It can receive and send k bits (say k=8) at a time in a streamed manner

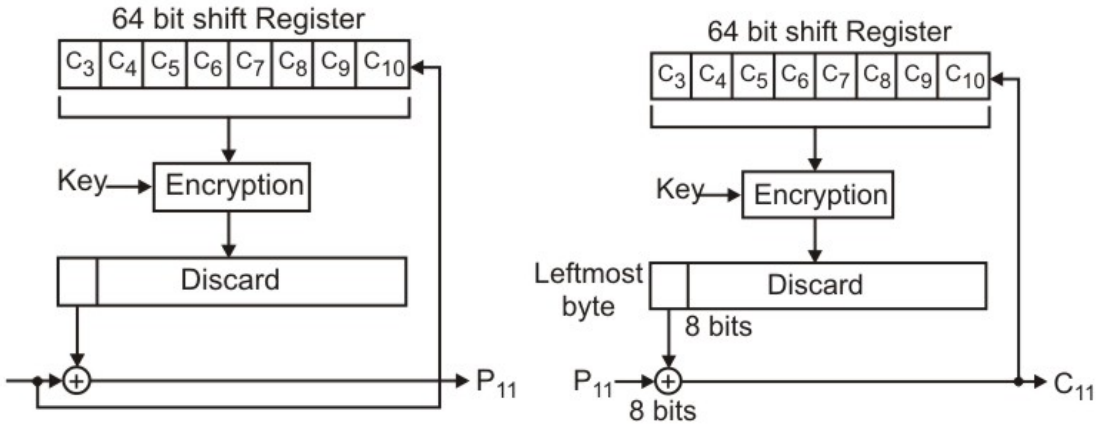

Figure 8.1.13 Cipher Feedback Mode (CFB) encryption technique

Output Feedback Mode (OFB)

The encryption technique of Output Feedback Mode (OFB) is shown in Fig. 8.1.14. Key features of this mode are mentioned below:

- OFB is also a stream cipher
- Encryption is performed by XORing the message with the one-time pad
- One-time pad can be generated in advance
- If some bits of the ciphertext get garbled, only those bits of plaintext get garbled
- The message can be of any arbitrary size
- Less secure than other modes

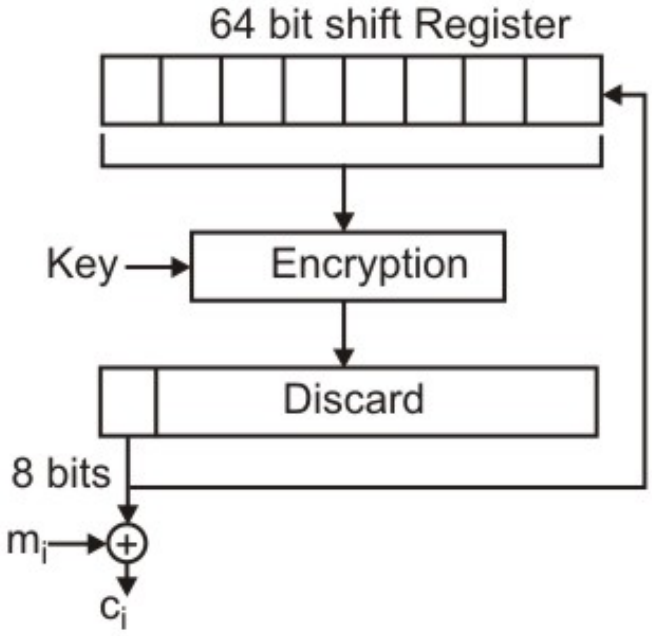

Figure 8.1.14 Output Feedback Mode (OFB) encryption technique

8.1.2.7 Triple DES

Triple DES, popularly known as 3DES, is used to make DES more secure by effectively increasing the key length. Its operation is explained below:

- Each block of plaintext is subjected to encryption by K1, decryption by K2 and again encryption by K1 in a sequence as shown in Fig. 8.1.15
- CBC is used to turn the block encryption scheme into a stream encryption scheme

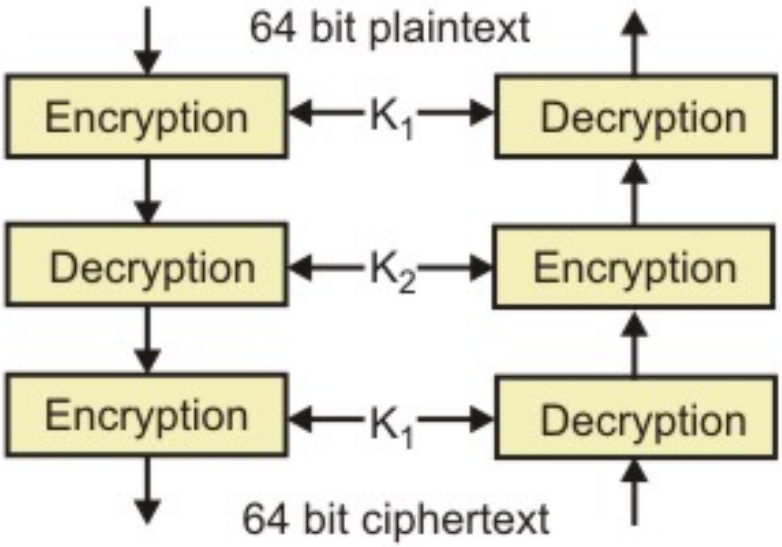

Figure 8.1.15 Triple DES encryption technique

8.1.3 Public key Cryptography

In public key cryptography, there are two keys: a private key and a public key. The public key is announced to the public, where as the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption as shown in Fig. 8.1.16.

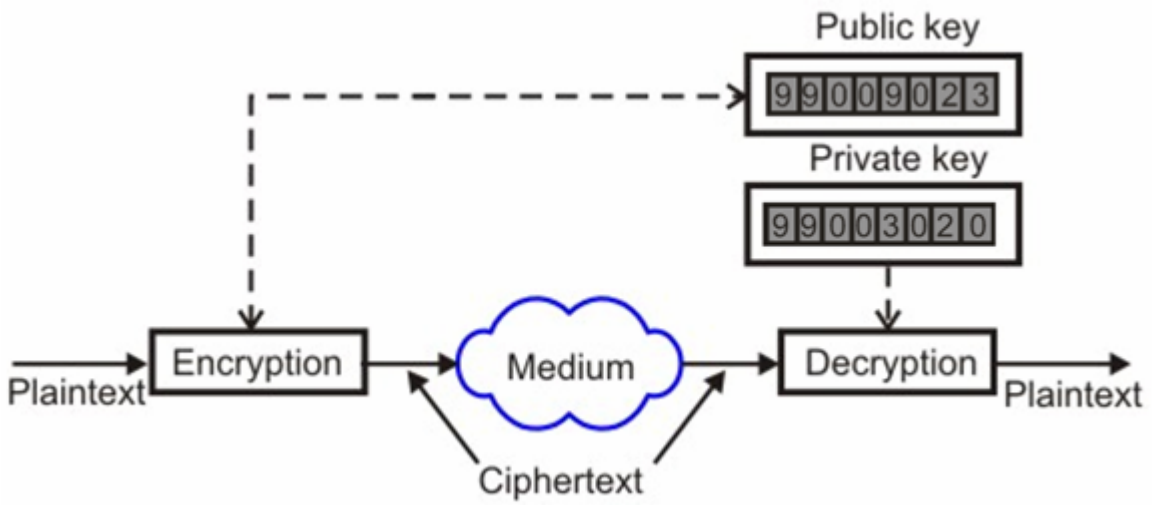

Figure 8.1.16 Public key encryption technique

- Advantages:
  - The pair of keys can be used with any other entity
  - The number of keys required is small
- Disadvantages:
  - It is not efficient for long messages
  - Association between an entity and its public key must be verified

8.1.3.1 RSA

The most popular public-key algorithm is the RSA (named after their inventors Rivest, Shamir and Adleman) as shown in Fig. 8.1.17. Key features of the RSA algorithm are given below:

- Public key algorithm that performs encryption as well as decryption based on number theory
- Variable key length; long for enhanced security and short for efficiency (typical 512 bytes)
- Variable block size, smaller than the key length
- The private key is a pair of numbers (d, n) and the public key is also a pair of numbers (e, n)
- Choose two large primes p and q (typically around 256 bits)
- Compute n = p x q and z = (p-1)x(q-1)
- Choose a number d relatively prime to z

- Find e such that e x d mod (p-1)x(q-1) = 1
- For encryption: C = Pe (mod n)
  For decryption: P = Cd (mod n)

Figure 8.1.17 The RSA public key encryption technique

Review Questions

1.What do you mean by encryption and decryption?

Ans: Encryption transforms a message (plaintext) into a form (ciphertext) unintelligible to an unauthorized person. On the other hand, decryption transforms an unintelligible (ciphertext) message into meaningful (plaintext) information by an authorized person.

2. What are the two approaches of encryption/decryption technique?

Ans: There are basically two approaches as follows:
One key technique (or symmetric encryption) – In this case the same key is used for encryption and decryption. Public key (or asymmetric encryption) – In this case the transmitting end key is known (or public), whereas the receiving end key is secret.

3. For n number of users, how many keys are needed if we use private and public key cryptography schemes?

Ans: For n users n(n-1)/2 keys are required in private key cryptography and 2n keys are required in public key cryptography.

4. How triple DES enhances performance compared to the original DES?

1.Ans: It was realized that the DES key length was too short to provide high security. Triple DES was used to make DES more secure by effectively increasing the key length. Here two keys are used in three stages.

5. Explain how RSA works.

Ans: The steps of RSA is as follows:
1.Choose two large primes p and q (typically around 256 bits)
2.Compute n = p x q and z = (p-1)x(q-1)
3.Choose a number d which is relatively prime to z
4.Find e such that e x d mod (p-1)x(q-1) = 1

For encryption: $C = P^e \pmod{n}$

For decryption: $P = C^d \pmod{n}$