Q1) Describe Using FIGURE only the S-DES Structure? Explain the Encryption process in S-DES?

ANSWER:

S-DES Structure can be described as follow:

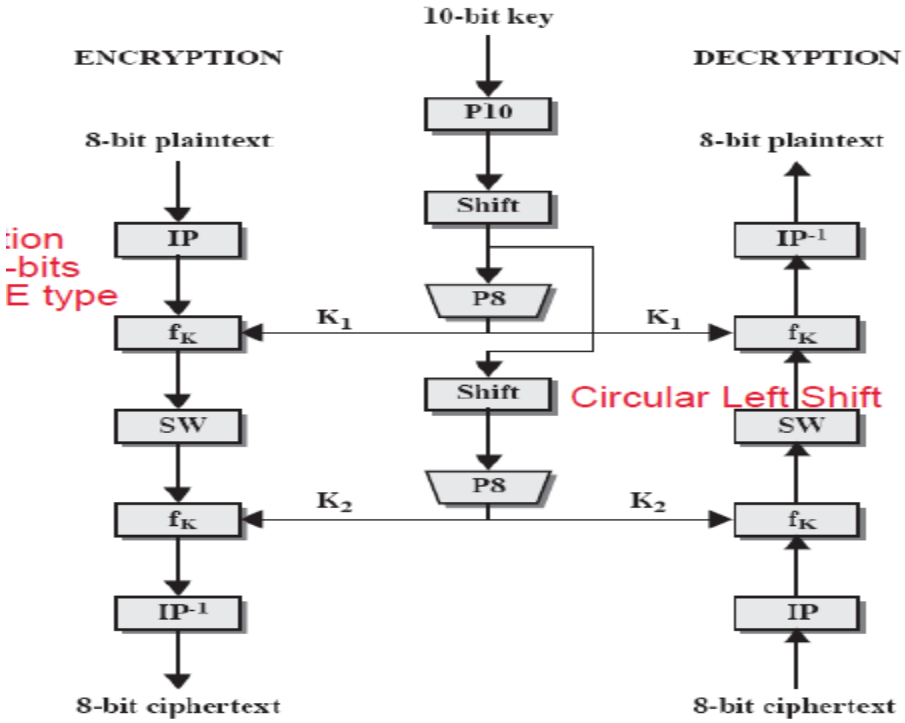

Figure 3-1. S-DES Scheme

Encryption process in S-DES can be explained as follow:

1. **Encryption:**

The encryption algorithm involves **five functions**:

a. An initial permutation (IP);

b. A complex functions labeled f_k which involves both permutation and substitution operations and depends on a key input a simple permutation function

c. Switches (SW) the two halves of the data;

d. The function f_k again, and

e. Finally a permutation function that is the inverse of initial permutation (IP^{-1}).

We can express the encryption algorithm as a composition of functions:

$$IP^{-1}.F_{K2}.SW.F_{K1}.IP$$

Which can be written as:

$$Ciphertext = IP^{-1}(F_{K2}(SW(F_{K1}(IP(Plaintext)))))$$

Q2) Consider that PlainText="11010011". Find the Cipher Text depends on the following FACTS:

- **CipherText = IP-1 (fK2 (SW (fk1 (IP (PlainText)))))**
- **SK=3412.**
- **Initial and Inverse Permutation as below:**

IP							
2	6	3	1	4	8	5	7

IP –1							
4	1	3	5	7	2	8	6

ANSWER:

Encryption:

$$\text{Ciphertext} = \mathbf{IP^{-1}}\ (f_{K2}\ (\mathbf{SW}\ (f_{k1}\ (\mathbf{IP}\ (\text{plaintext})))))$$

Encryption involves the sequential application of five functions.

Initial and Final Permutations

The input to the algorithm is an 8-bit block of plaintext, which we first permute using the IP function:

IP							
2	6	3	1	4	8	5	7

This retains all 8 bits of the plaintext but mixes them up.

Consider the plaintext to be **11010011**.

IP= 10010111

1	1	0	1	0	0	1	1
8	7	6	5	4	3	2	1
2	**6**	**3**	**1**	**4**	**8**	**5**	**7**
1	0	0	1	0	1	1	1

Permuted output = **10010111**

At the end of the algorithm, the inverse permutation is used:

IP –1							
4	1	3	5	7	2	8	6

The Function f_k

The most complex component of S-DES is the function f_k, which consists of a combination of permutation and substitution functions. The functions can be expressed as follows. Let L and R be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to f K, and let F be a mapping (not necessarily one to one) from 4-bit strings to 4-bit strings. Then we let

Fk# =(L XOR F(R,SK),R)

Example: L and R (Right and Left of BITS)

Let (IP (plaintext)= 10010111

Let K1=(**10010111**) and

Suppose **F(0111,SK)** and (**SK=3412**)=**1011 (this 4-bits).**

Therefore:

Fk1 =(1001 XOR 1011,0111)

=(00100111)

3 The Switch Function

The function f K only alters the leftmost 4 bits of the input. The switch function (SW) interchanges the left and right 4 bits

Example:

=SW (00100111)= (01110010)

Fk2=(01110010) and SK=3412

Fk2 =(L XOR F(R,SK),R)

Fk2 =(0111 XOR F(0010,3412),0010)

Fk2 =(0111 XOR 0001,0010)

Fk2 =(01100010) 8-bits

IP –1							
4	1	3	5	7	2	8	6

IP-1=00001101

Therefore the ciphertext=”00001101”

Q3) Describe the steps of generating keys in RSA Public-Key Algorithm? Find the Private and Public keys for the following prime pair numbers (11, 19) of Q and P respectively?

ANSWER:

Key generation:

1. Choose P,Q.
2. Compute N=P X Q.
3. Compute Euler(N)= (P-1)X(Q-1).
4. Choose (e) where:
    a. 1<e<Euler(N).
    b. GCD(e,Euler(N)=1.
5. Calculate (d):
    a. **d**Xe=??mod Euler(N)=**1**
6. the generated KEYS:
    a. KU (e,N).
    b. KR (d,N).

Encryption: C= M^e MOD N. Decryption: M=C^d MOD N.

Compute Private and Public KEYS:

Step1: Set p and q

Choose p and q as prime numbers

p value=19

q value=11

SET P AND Q

N = p * q : 209

Phi(N) = (p - 1) * (q - 1) : 180

Step2: Choose public key e (Encryption Key)

Choose e from below values
(7,11,13,17,19,23,29,31,37,41,43,47,49,53,59,61,67,71,73,77,79,83,89,91,97,101,103,107,109,113,119,121,127,131,133,137,139,143,149,151,157,161,163,167,169,173,179)

Let e=7 therefore **Public key is (e , n) = 7, 209**

Step3: Choose private key d (Decryption Key)

Choose d from below values (103). **Private key is (d , n) = 103, 209.**