S-DES Problem

Using the 10 bit key **1 0 1 0 0 0 0 1 1 0**

Encrypt the following 8 bit plaintext using the Simplified DES (S-DES) cipher **1 0 0 0 0 1 1 0**

$$\text{ciphertext} = IP^{-1}\left(f_{K_2}\left(SW\left(f_{K_1}\left(IP(\text{plaintext})\right)\right)\right)\right)$$

where

$$K_1 = P8\left(\text{Shift}\left(P10(\text{key})\right)\right)$$

$$K_2 = P8\left(\text{Shift}\left(\text{Shift}\left(P10(\text{key})\right)\right)\right)$$

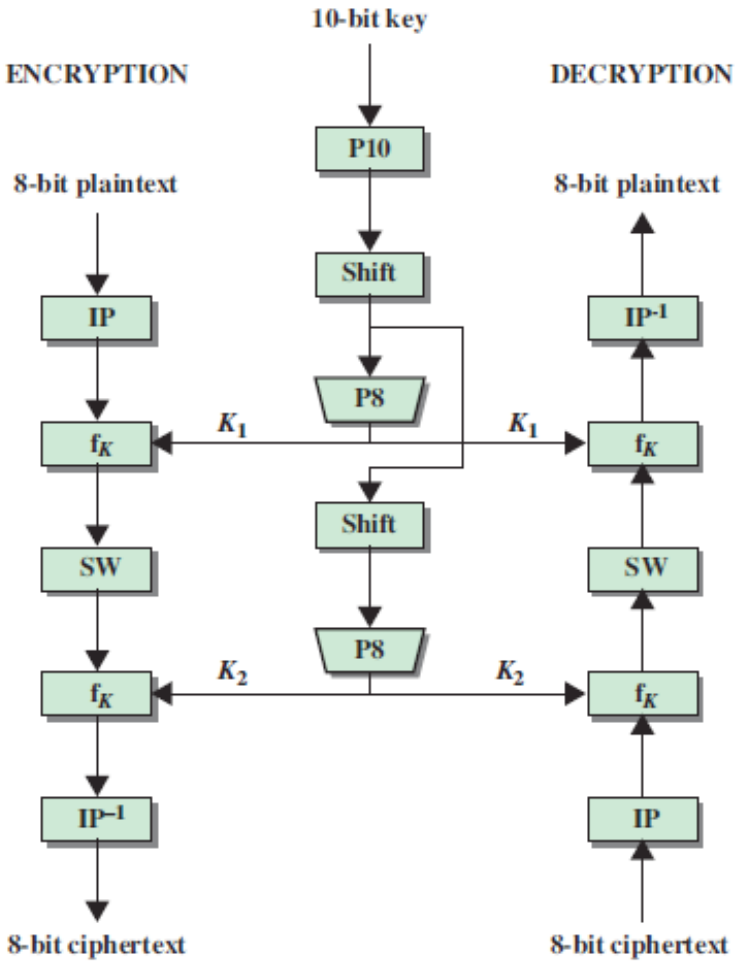

Figure G.1 Simplified DES Scheme

Key Generation

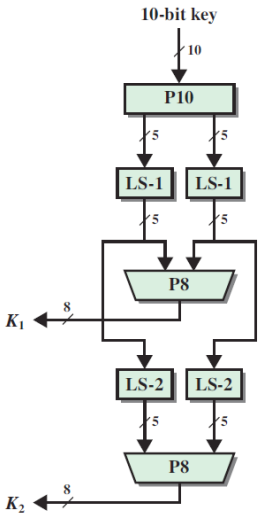

Figure G.2 Key Generation for Simplified DES

The P10 permutation is defined as

P10									
3	5	2	7	4	10	1	9	8	6

P8 is given by

P8							
6	3	7	4	8	5	10	9

K1 =

K2 =

S-DES Encryption

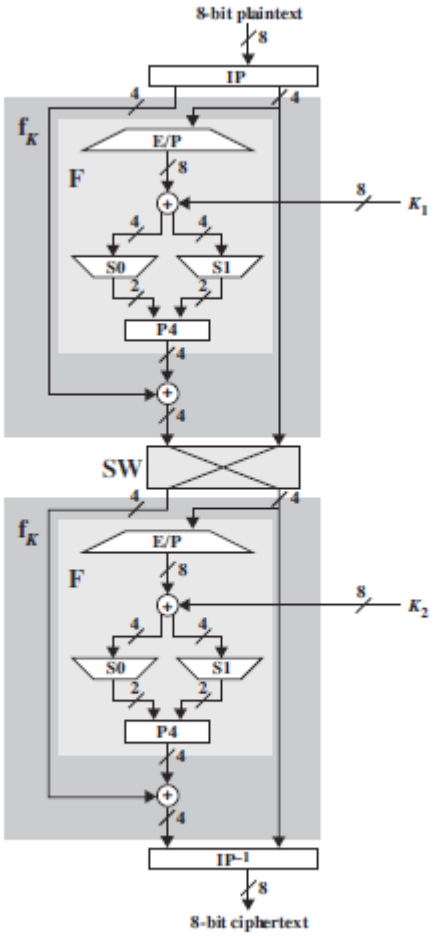

Figure G.3 Simplified DES Encryption Detail

The initial permutation IP is defined as (from which IP^{-1} can easily be deduced)

IP							
2	6	3	1	4	8	5	7

E/P is defined as

E/P							
4	1	2	3	2	3	4	1

The S boxes are given as

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

And P4 is defined as

P4			
2	4	3	1

Ciphertext =