LAB 3

DUE 02/23/2019 11:59:59 PM

Instructions

Data Standard Encryption (DES) lab. In this lab you would be performing hand calculations for SIMPLIFIED DES. This lab is to give you the opportunity to learn the actual steps by hand and to get the gist of the DES technique in a simplified form. Please follow the diagrams carefully and follow each step.

Assignment (50 points total)

Part I: Key Generation for Simplified DES

1. Obtain from your instructor a unique 10-bit key

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

Part II: Simplified DES Encryption

2. Obtain from your instructor a unique 8-bit plain text
3. Start going through the steps as described on the diagrams to encrypt your message
4. Once you have encrypted the message! You are done. ☺

IP							
2	6	3	1	4	8	5	7

E/P							
4	1	2	3	2	3	4	1

LAB 3

DUE 02/23/2019 11:59:59 PM

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

P4			
2	4	3	1

IP^{-1}							
4	1	3	5	7	2	8	6

Ciphertext

LAB 3

DUE 02/23/2019 11:59:59 PM

Round 1	
Plaintext	<Insert Last two ID digits>
Initial Permutation	
Expansion Permutation Result	
XOR w/ Key1 Result	
S_0 Box Result	
S_1 Box Result	
S_0 & S_1 Combined Result	
Permutation 4 Result	
XOR w/ Left 4-bits Result	
8-bit Result	
8-bit Result Swap	

LAB 3

DUE 02/23/2019 11:59:59 PM

Round 2	
Plaintext	<Insert Last two ID digits>
Initial Permutation	
Expansion Permutation Result	
XOR w/ Key1 Result	
S_0 Box Result	
S_1 Box Result	
S_0 & S_1 Combined Result	
Permutation 4 Result	
XOR w/ Left 4-bits Result	
8-bit Result	
Initial Permutation^{-1}	

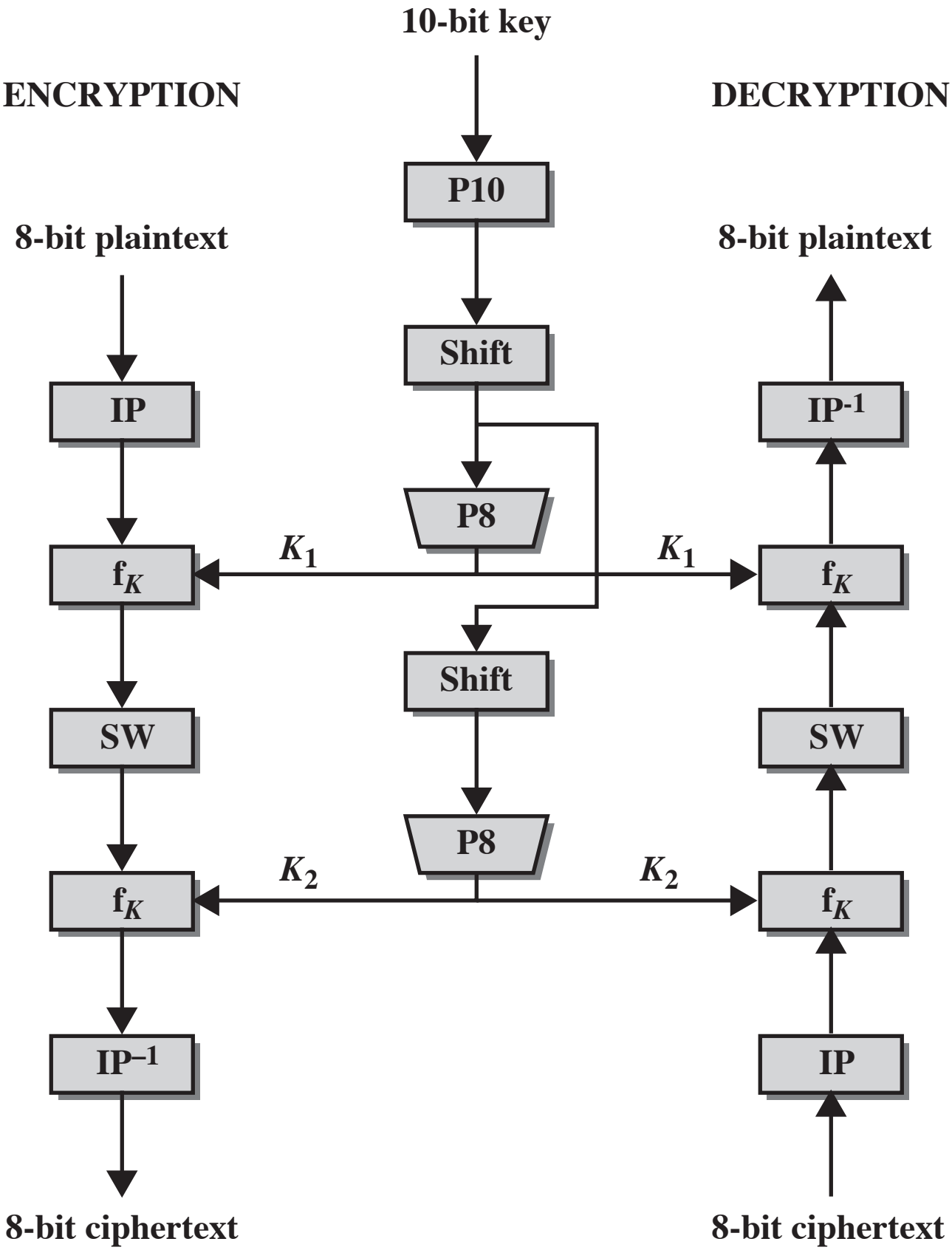

Figure G.1 Simplified DES Scheme

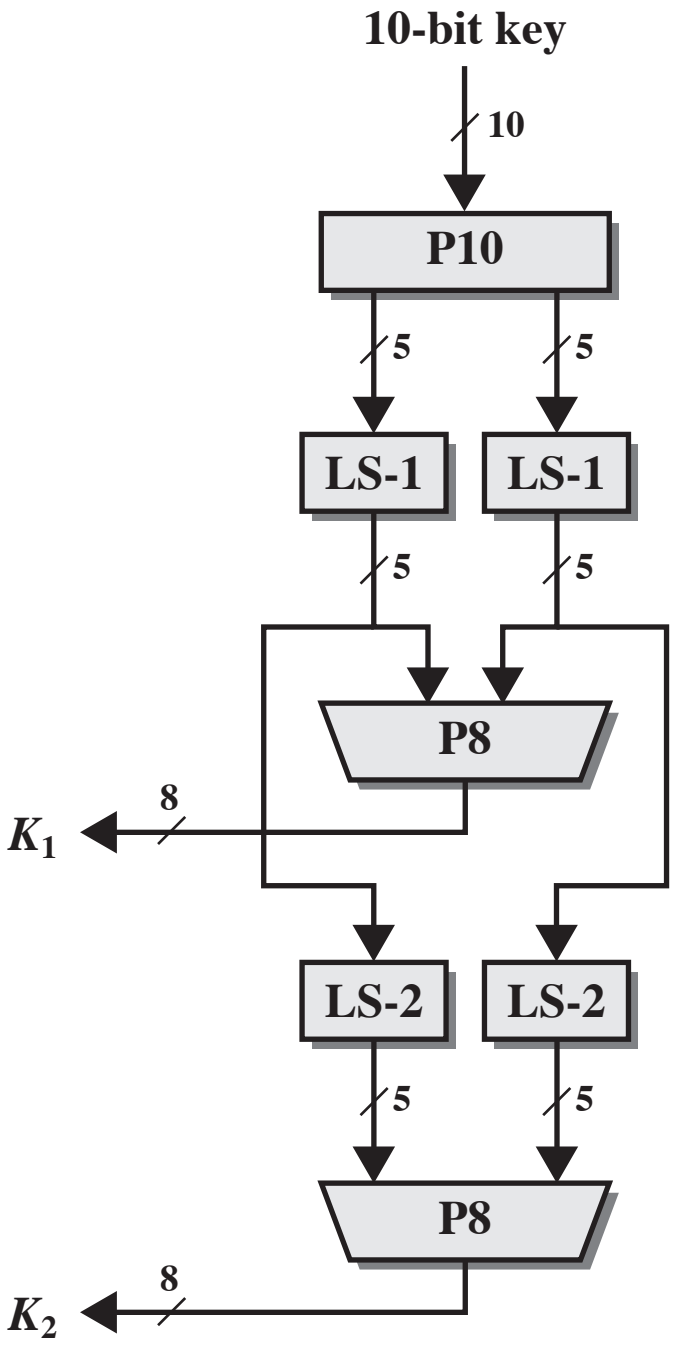

Figure G.2 Key Generation for Simplified DES

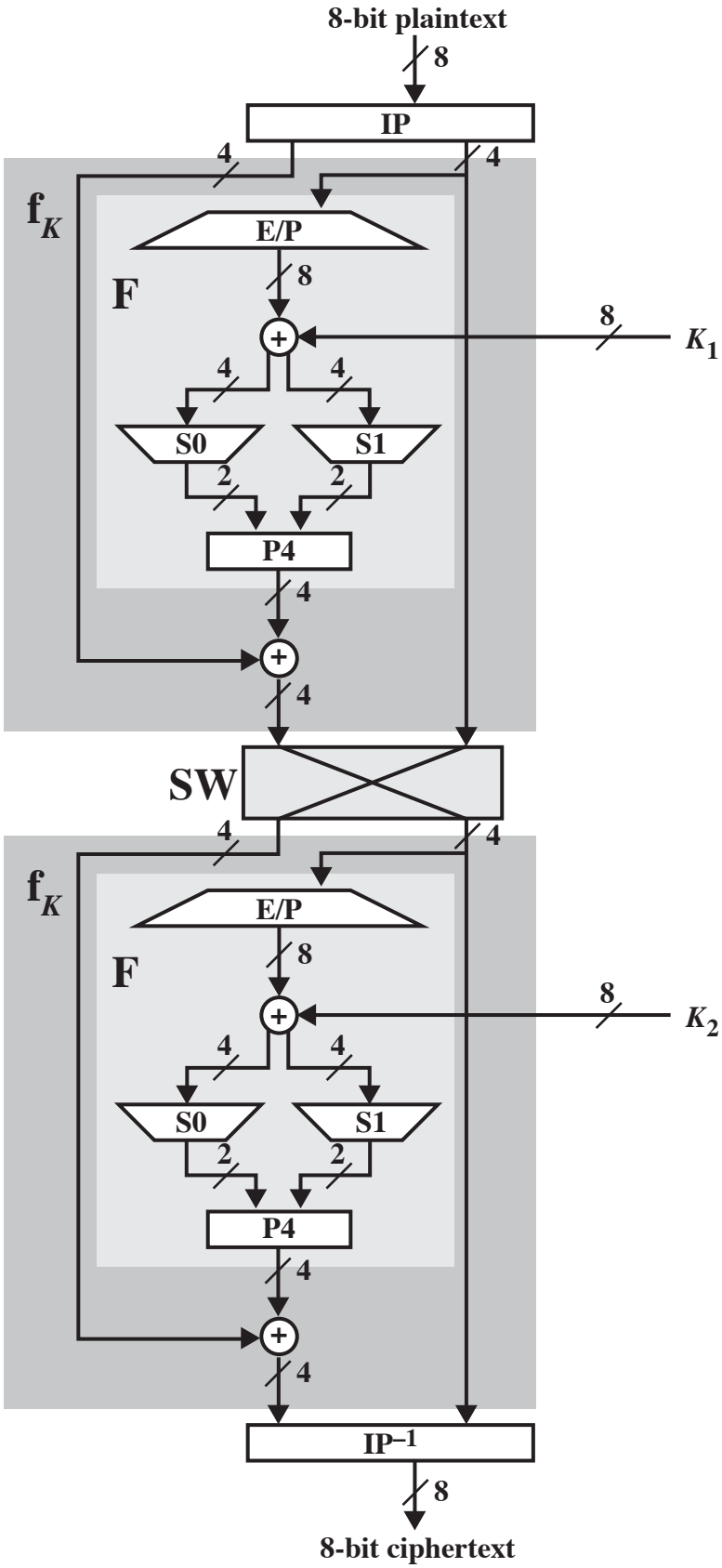

Figure G.3 Simplified DES Encryption Detail