Block Cipher

Eighth lecture(cont.)

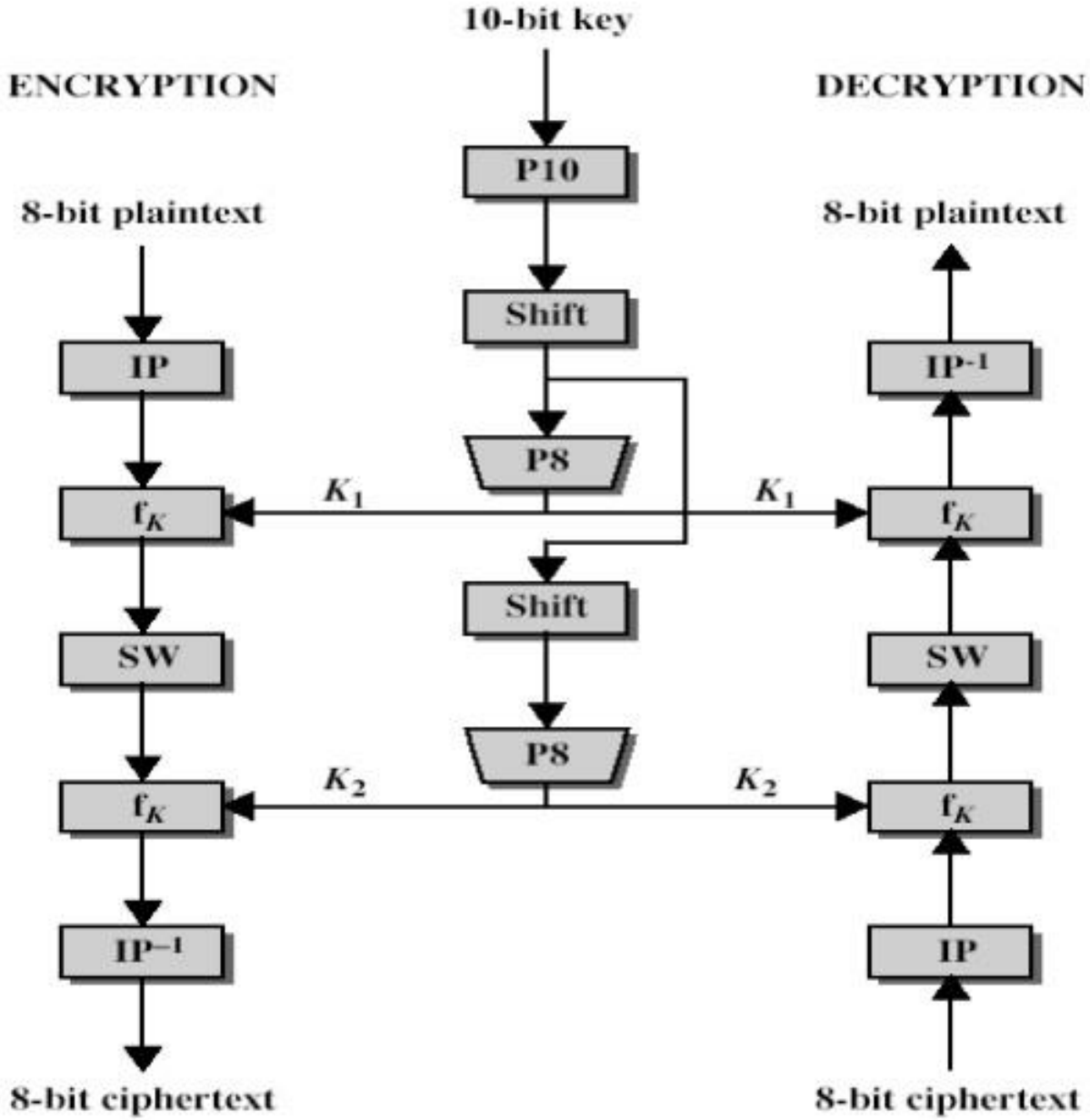
By: Assist Prof. Dr. Saja J. Mohammed

2024-2025

Simplified Data Encryption Standard (S-DES)

- **Simplified Data Encryption Standard** is a simple version of Data Encryption Standard which discovered in 1970's.
- It was developed for educational purpose so that understanding DES can become easy.
- It has a **10-bit key and 8-bit plaintext**.
- It is a block cipher algorithm and uses a symmetric key for its algorithm i.e. they use the same key for both encryption and decryption.
- It has **2 rounds** for encryption which use two different keys.
- S-DES is a type of product block cipher.
- **Product cipher** is a cryptographic technique that combines multiple simple transformations to encrypt or decrypt data. It operates on blocks of data and uses both substitution and permutation methods. Product ciphers are designed to enhance encryption strength through complexity

S-DES


10-bit key
ENCRYPTION
DECRYPTION
P10
8-bit plaintext
8-bit plaintext
Shift
IP
IP-1
P8
K1
K1
fK
fK
Shift
SW
SW
P8
K2
K2
fK
fK
IP-1
IP
8-bit ciphertext
8-bit ciphertext

P- Box in S-DES

S-DES has 5 types of permutation box:

- ✓ IP and IP^{-1} (Initial permutate, ***straight*** *8bit)*
- ✓ P10 **(*straight*** *permutate 10 bits)*
- ✓ P4 (***straight*** *permutate 4bits)*
- ✓ P8 (***compression*** permutate 10 bits ➔ 8bits)
- ✓ EP (***expanded*** permutate 4bits ➔ 8 bits)

P10 table

Input	1	2	3	4	5	6	7	8	9	10
Output	3	5	2	7	4	10	1	9	8	6

P8-Table

Input	1	2	3	4	5	6	7	8	9	10
Output	6	3	7	4	8	5	10	9		

IP table

Input	1	2	3	4	5	6	7	8
Output	2	6	3	1	4	8	5	7

P 4 Table

Input	1	2	3	4
Output	2	4	3	1

E.P Table

Input	1	2	3	4				
Output	4	1	2	3	2	3	4	1

S-box in S-DES

S-0

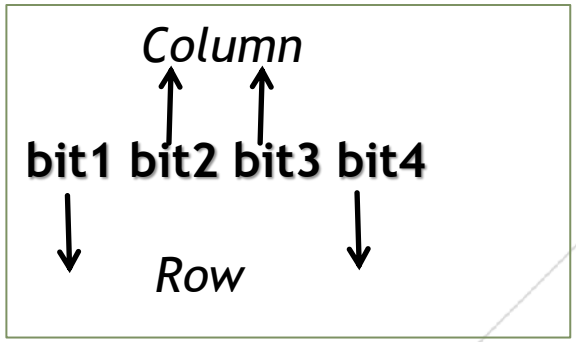
Col	0	1	2	3
Rows				
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S-1

Col	0	1	2	3
Rows				
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

4-bit input: bit1,bit2,bit3,bit4
2-bits Output

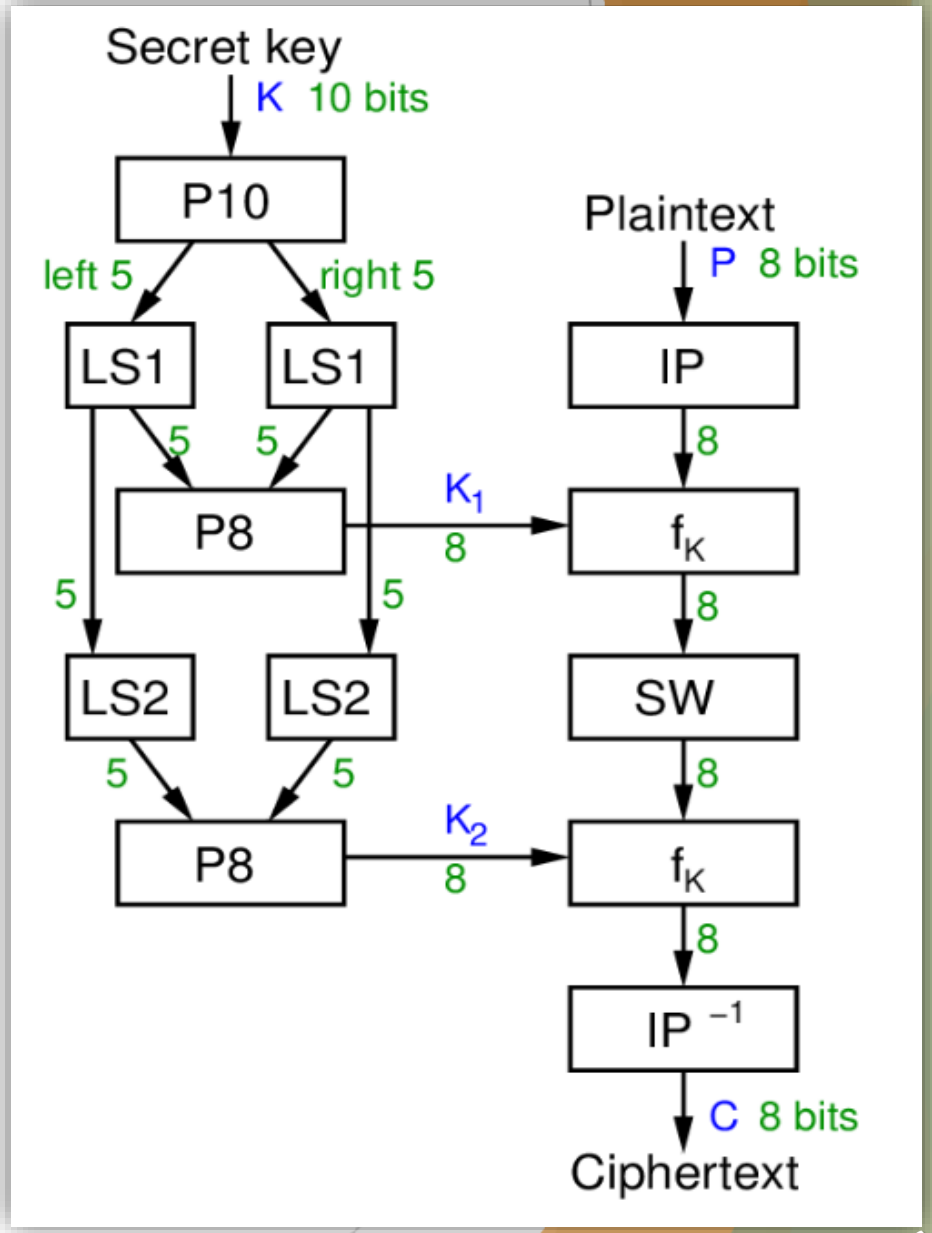
bit1 ,bit4 specifies row (0, 1, 2 or 3 in decimal)
bit2 , bit3 specifies column
ex.
1010
That mean row 2 and column 1 ➔ output is 10 (in S0)
➔ output is 00 (in S1)



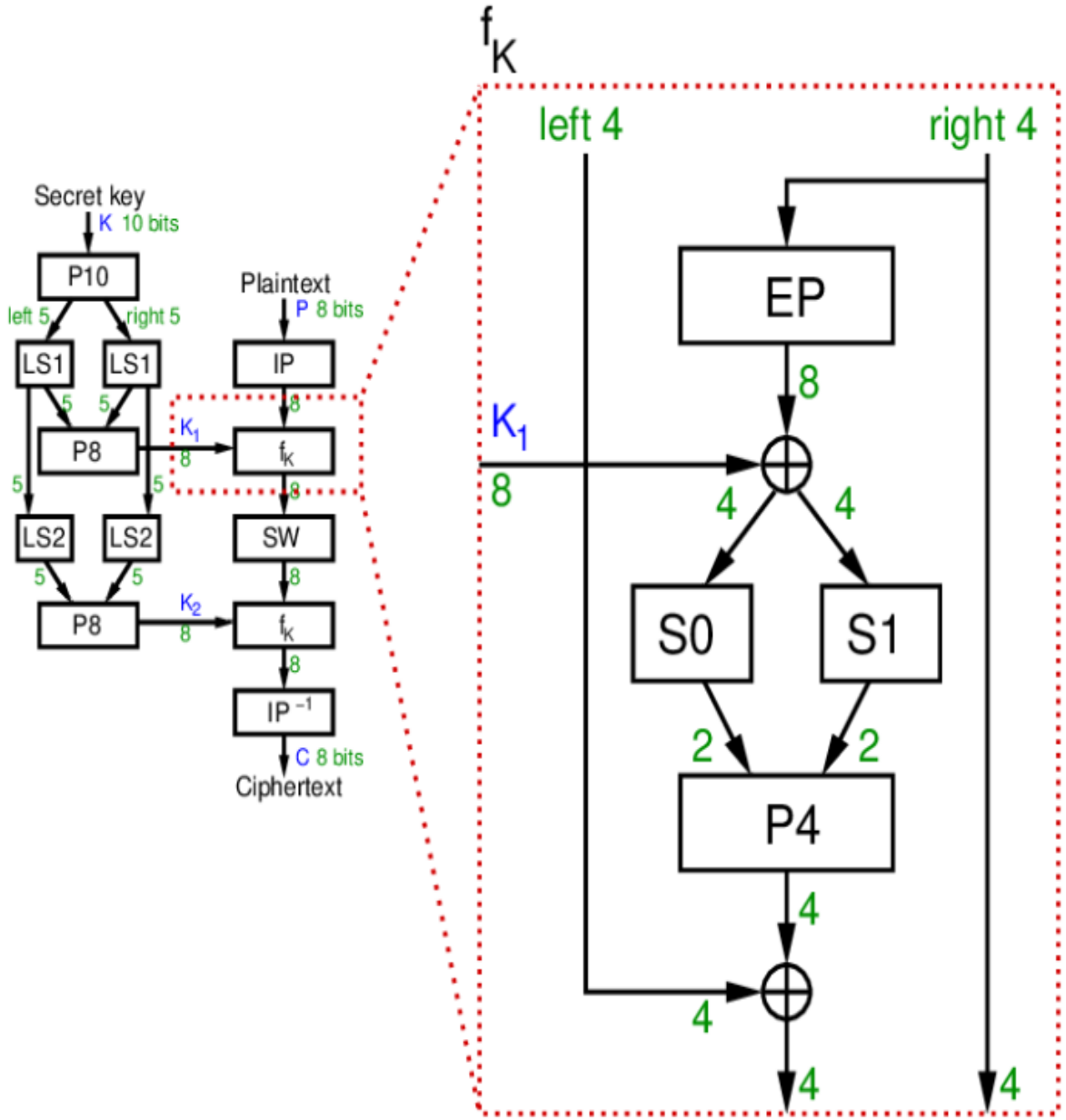
S-DES Encryption/ Decryption

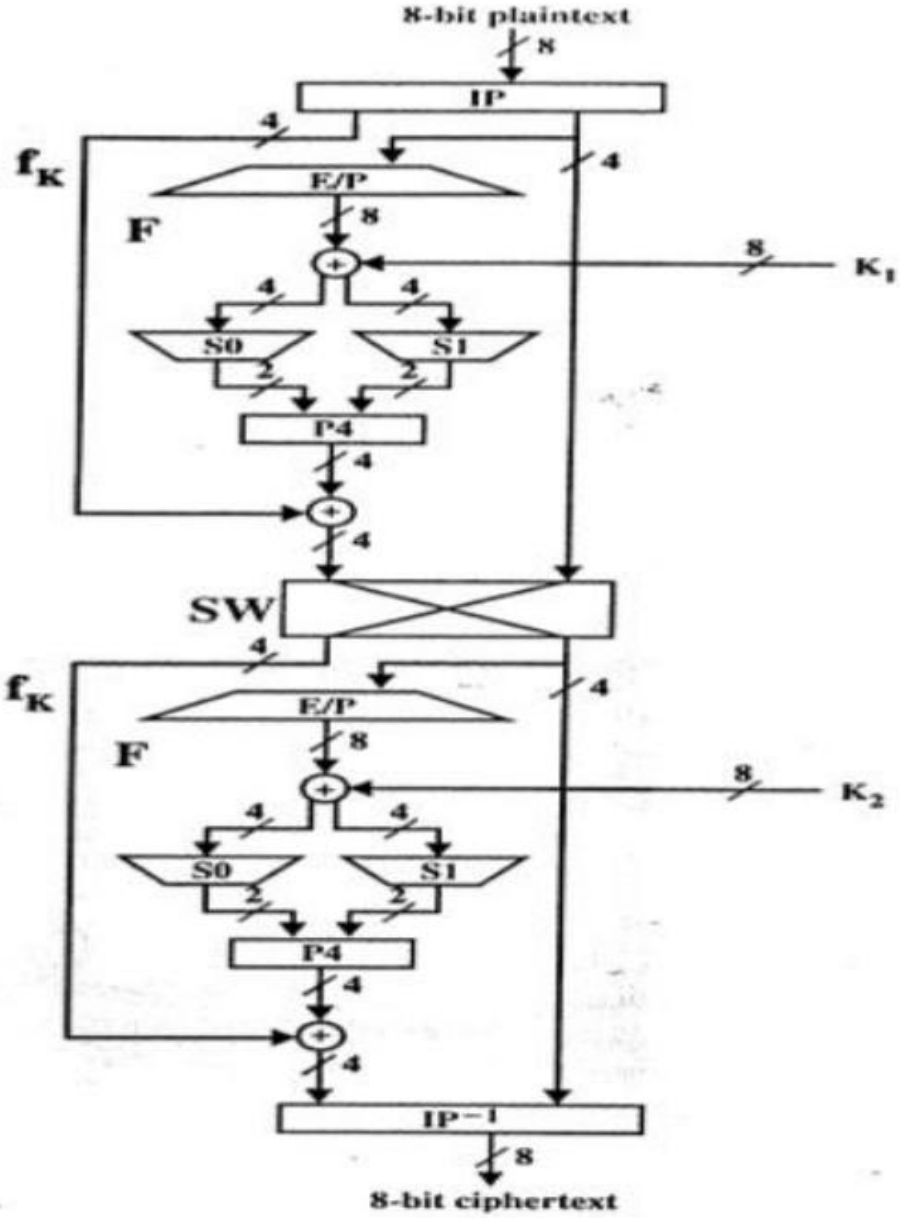
- **The encryption algorithm involves five functions:**

1. An initial permutation (IP)
2. Applying the round function using round key K1 (this function involves both permutation and substitution operations and depends on a key input)
3. Switches (SW) the two halves of the data
4. Applying the round function using round key K2
5. A permutation function that is the inverse of the initial permutation (IP^{-1}).



S-DES Round Function Details

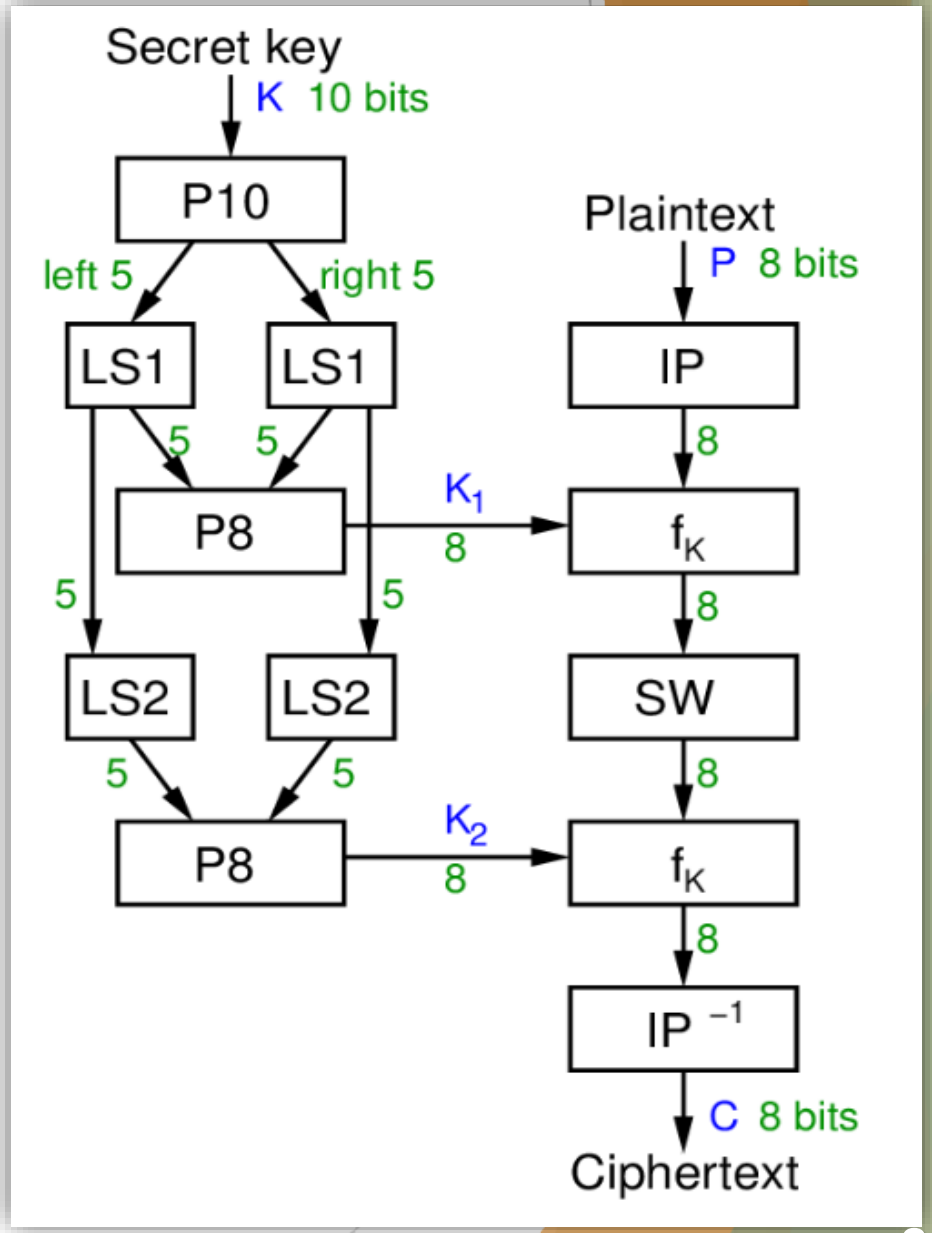




Simplified DES Scheme Encryption Detail.

S-DES Key Generation

- **Step 1:** Select a random key of 10-bits (shared between sender and receiver)
- **Step 2:**
  Put this key into P10 Table and permute the bits.
- **Step 3:** Divide the key into two halves, left half and right half;
- **Step 4:** Apply the one bit Round Shift **(LS1)**on each half
  Step 5: Combine both halve of the bits, right and left and Put them into the P8 table.
- **Step6:**
  Generate the second key(go in **step 4** copy both resulted halves, then apply two Round Shift**(LS2)**, combine resulted halves and input the result to P8 table

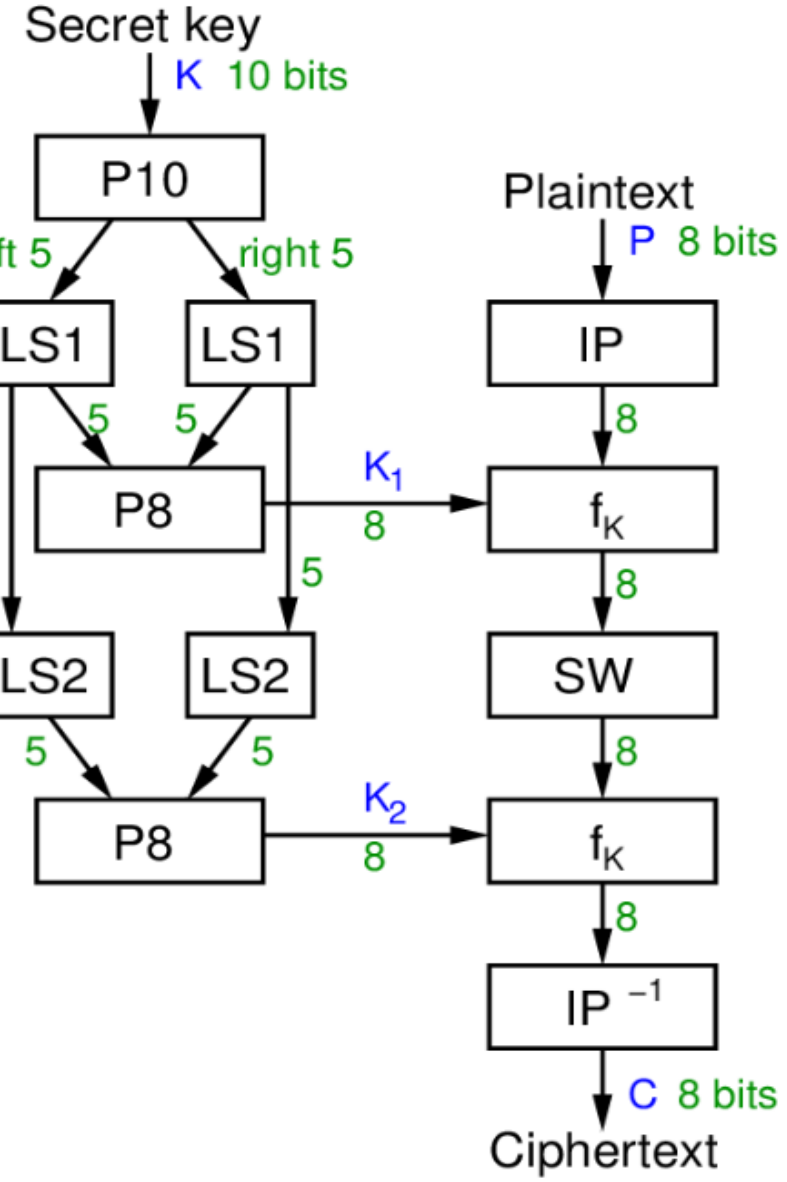


S-DES Key Generation example

- **Step 1:**
- Select a random key of 10-bits (shared between sender and receiver)
- Ex. :**1010000010**
- **Step 2:** Put this key into P10 Table and permute the bits.

Input	1	2	3	4	5	6	7	8	9	10
Output Should be	3	5	2	7	4	10	1	9	8	6

Input	1	0	1	0	0	0	0	0	1	0
Output	1	0	0	0	0	0	1	1	0	0



Key: 1000001100

S-DES Key Generation example

- **Step 3:** Divide the key into two halves, left half and right half;

  Left {1 0 0 0 0} | right {0 1 1 0 0}

- **Step 4:** Apply the one bit Round shift on each half:

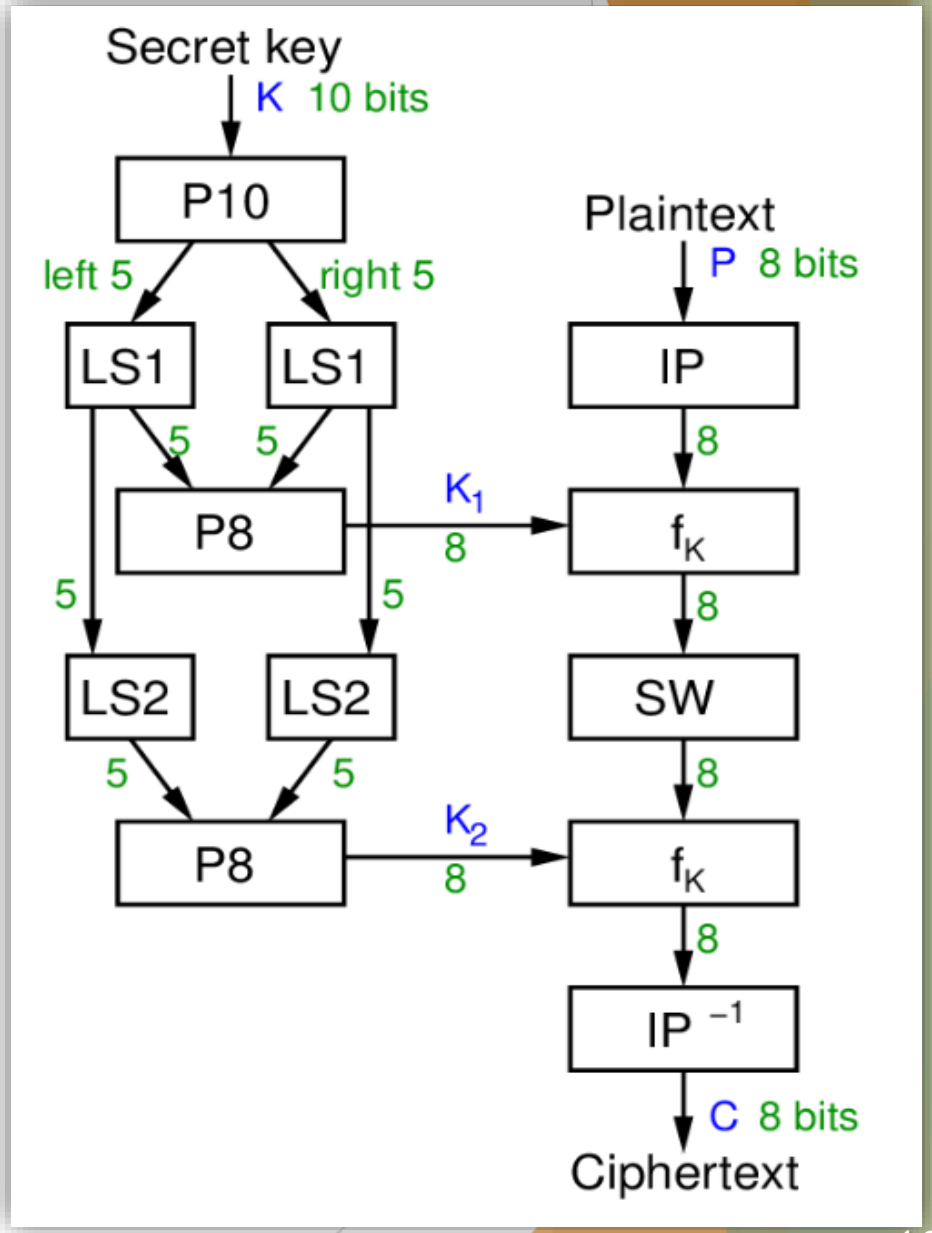
  Before round shift: {10000} | {01100}

  After round shift: {00001} | {11000}

- The output will be: {0 0 0 0 1} {1 1 0 0 0}
- **Step 5:**
- Combine both halve of the bits, right and left and put them into the P8 table. That will be the K1 or First key.
- Input key: 0 0 0 0 1 1 1 0 0 0 The output and K1 or key One will be: **K1=1 0 1 0 0 1 0 0 (8 bit)**

P8-Table

Input	1	2	3	4	5	6	7	8	9	10
Combine-bits	0	0	0	0	1	1	1	0	0	0
Output Should be	6	3	7	4	8	5	10	9		
Output bits	1	0	1	0	0	1	0	0		



S-DES Key Generation example

- **Step6:**
  Generate the second key(go in step 4 copy both resulted halves, then apply two round shift, combine resulted halves and input the result to P8 table

  00001 11000 ➔ 00100 00011

  (0010000011) input to p8 table ➔ 0010000011 (the output)

- The resulted key (key 2) will be : **0 1 0 0 0 0 1 1 (8 bit)**

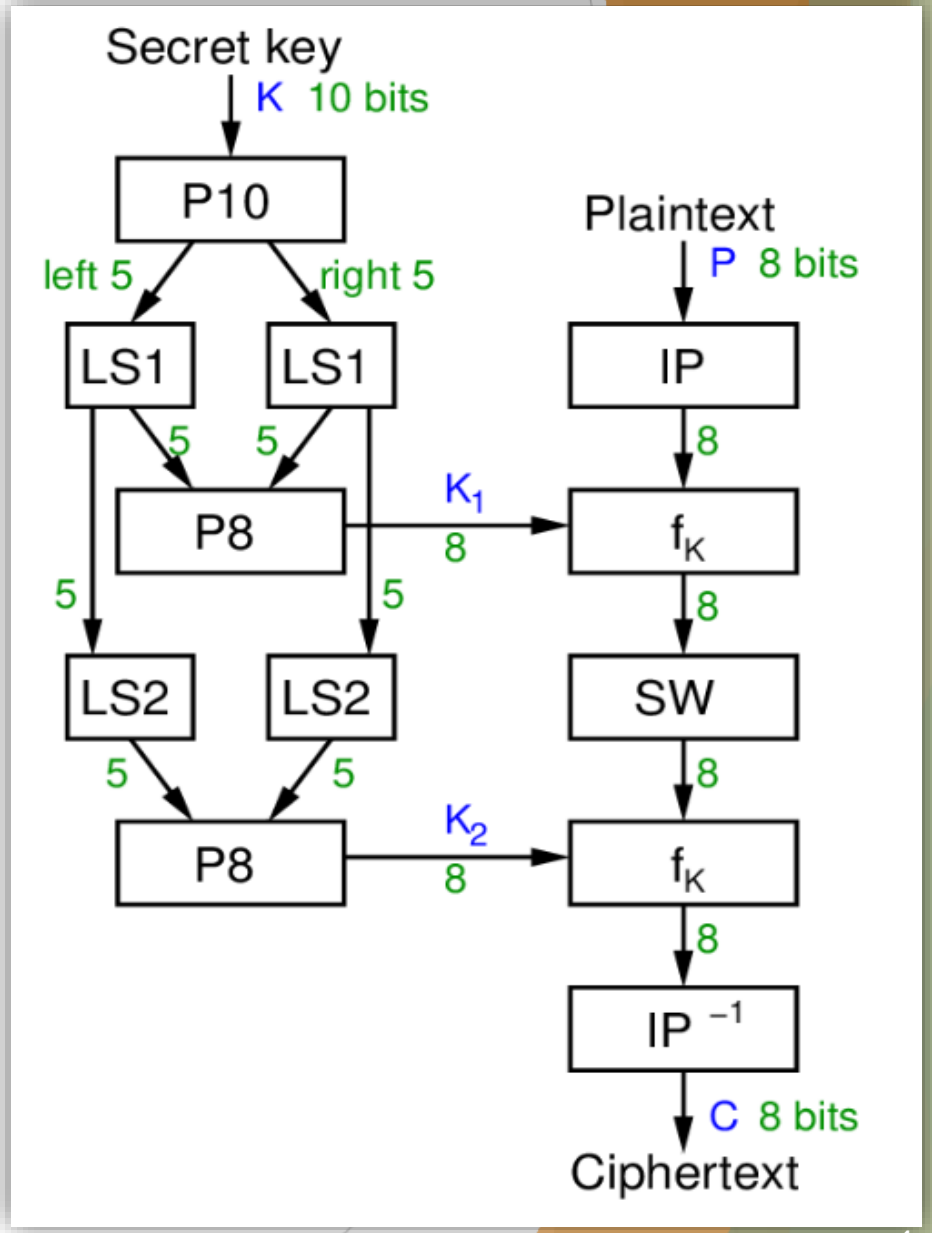
The generated keys are:

K1: 10100100

K2: 01000011

P8-Table

Input	1	2	3	4	5	6	7	8	9	10
Combine-bits	0	0	0	0	1	1	1	0	0	0
Output Should be	6	3	7	4	8	5	10	9		
Output bits	1	0	1	0	0	1	0	0		



S-DES Summary (properties)

- Block size: 8 bits and key size :10 bits
- Rounds: 2
- Round key: 2 round key each of size 8 bits
- S-Boxes: 2
- Permutations types: 5
  - ✓ P10 (*straight permutate 10bits)*
  - ✓ P8 (compression permutate 10 bits ➔ 8bits)
  - ✓ P4 (*straight permutate 4bits)*
  - ✓ IP and IP^{-1} (Initial permutate, *straight 8bit)*
  - ✓ EP (expanded permutate 4bits ➔ 8 bits)

S-DES Summary

- It is Educational encryption algorithm.
- **It is a type of product cipher.**
- S-DES expressed as functions:
  - ciphertext = IP-1(f K2(SW(fK1(IP(plaintext)))))
  - plaintext = IP-1(f K1(SW(fK2(IP(ciphertext)))))
- Brute force attack on S-DES **is easy** since only 10-bit key.
- If know plaintext and corresponding ciphertext, can we determine key? ***Very hard.***
- The general design of S-DES follows the same principles as DES, although the algorithm parameters differ.

- Find the result of the following:
- 1. GCD(35, 127)
- 2. $7^{-1}\ mod\ 3$