Cryptography ECE5632 - Spring 2024

Lecture 3B

Dr. Farah Raad

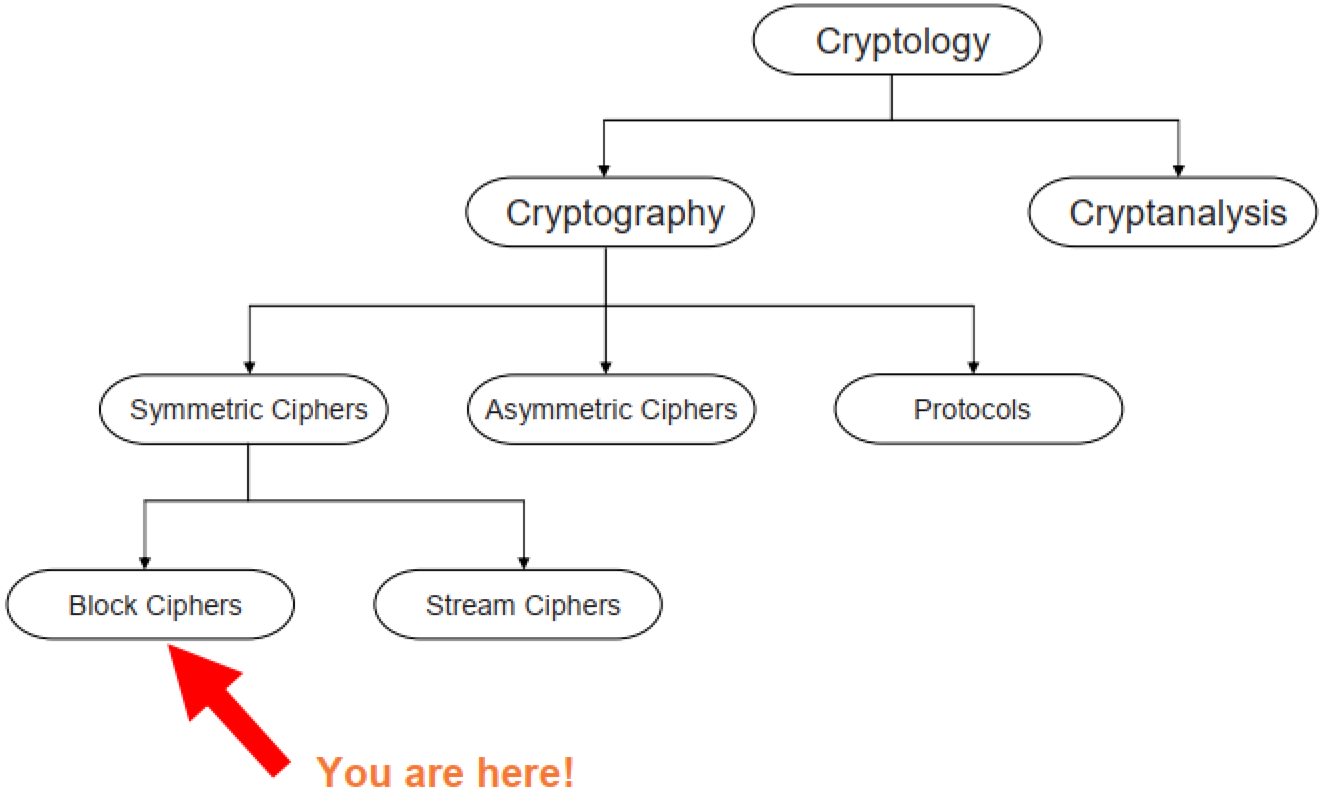
Lecture Topic

Simplified DES (SDES) & DES

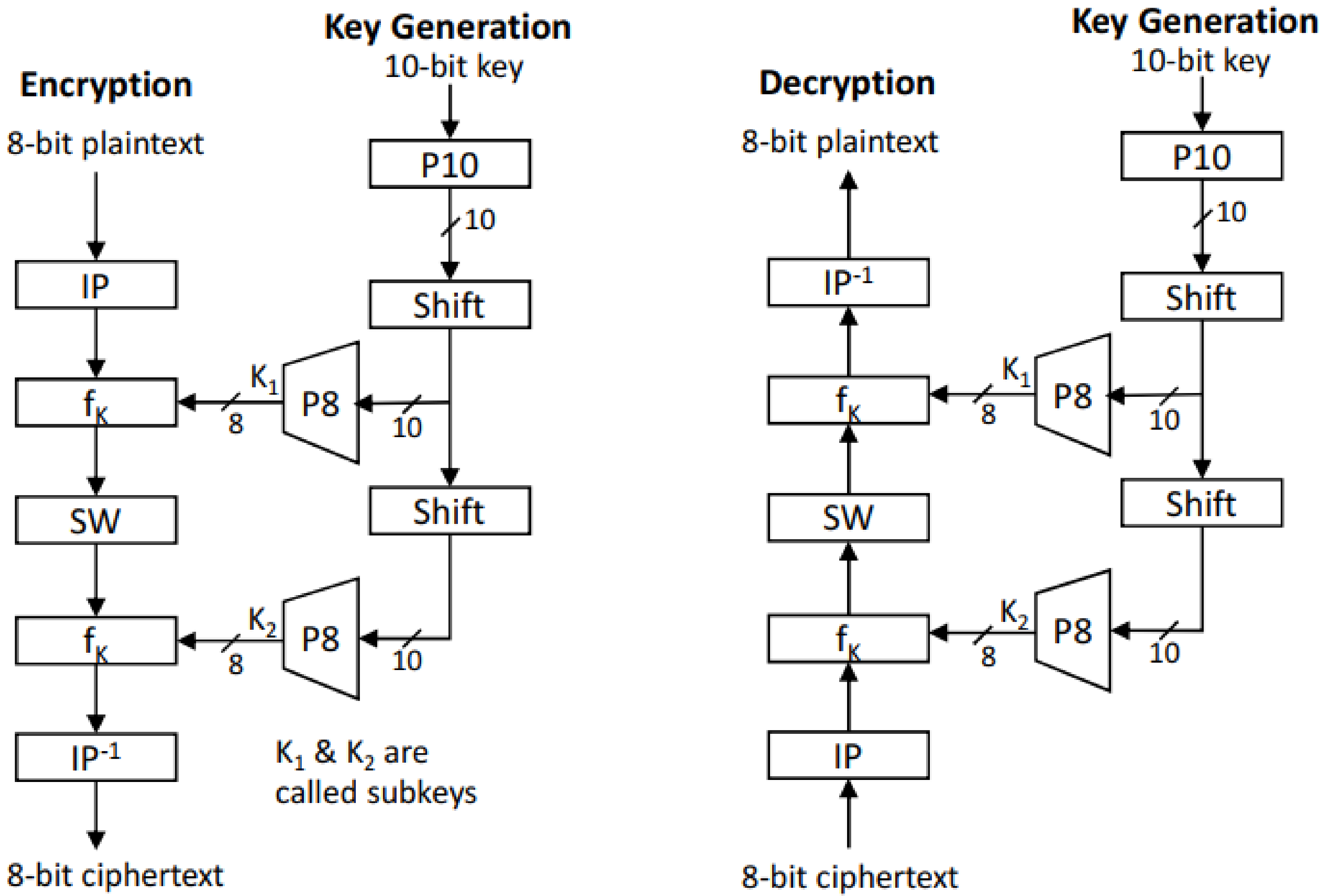
Simplified DES (SDES)

- Designed by Professor Edward Schaefer, for educational purposes.
- Similar properties and structure as DES (with much smaller parameters).
- The use of multiple stages of permutation and substitution results in a more complex algorithm, which increases the difficulty of cryptanalysis.

Classification of S-DES & DES in the Field of Cryptology



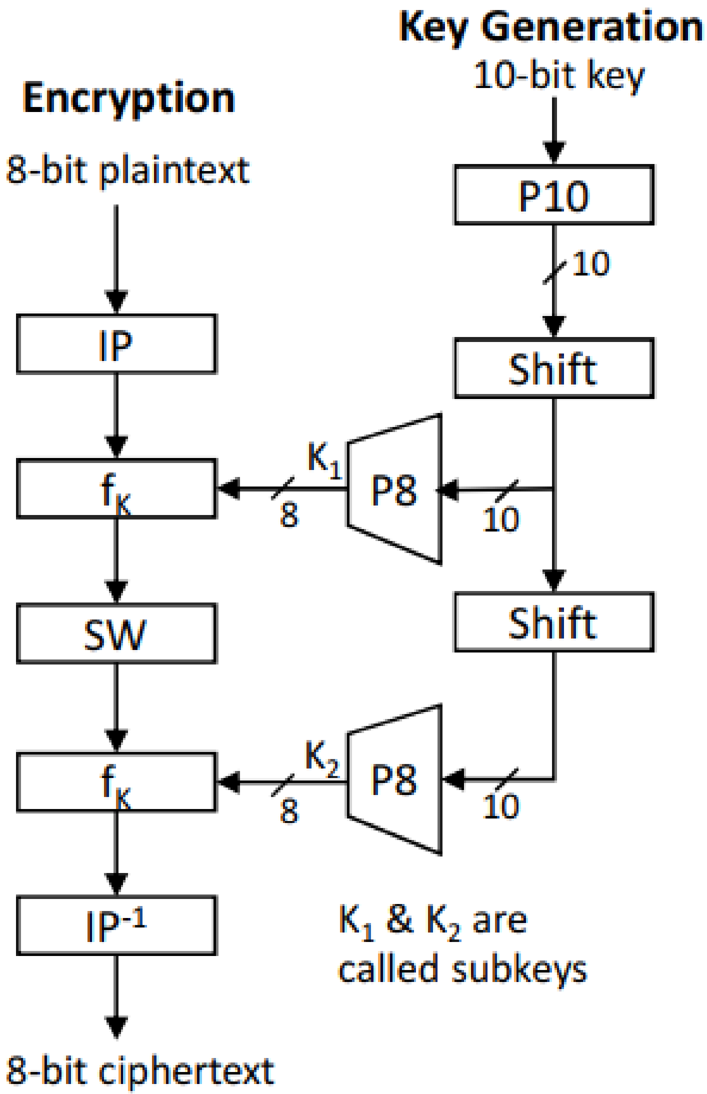
SDES: Overview



Encryption

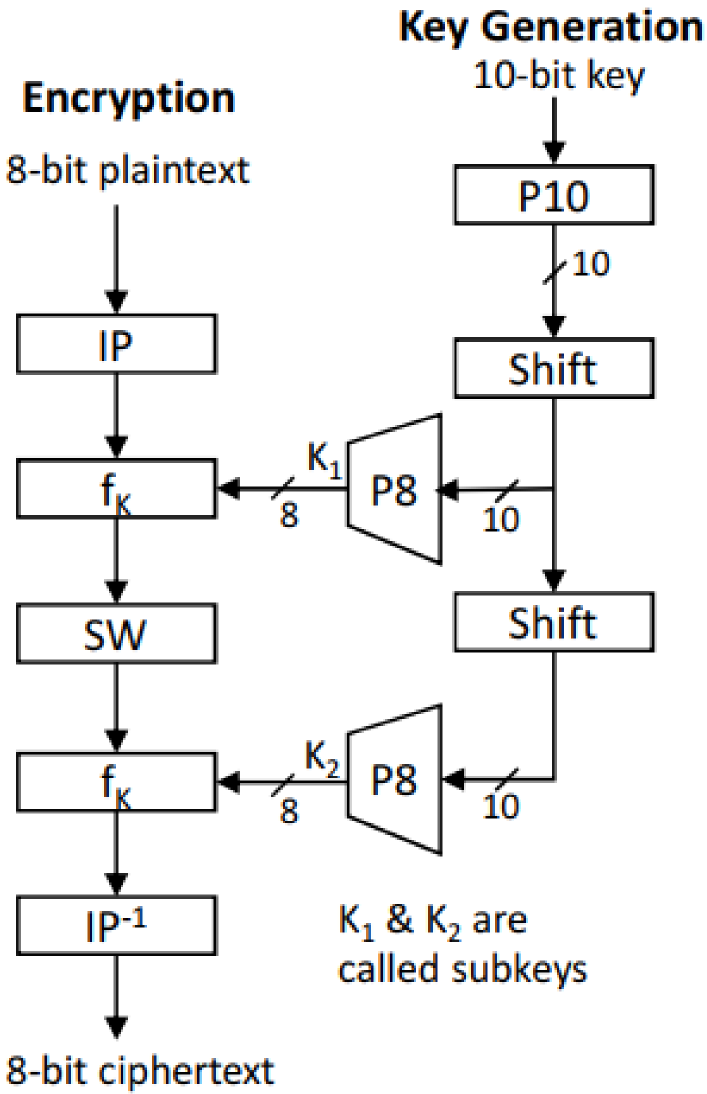
The encryption algorithm involves five functions:

1. Initial permutation (IP)
2. Complex function labeled ($\mathrm{f_k}$): which involves both permutation and substitution operations and depends on a key input.
3. Simple permutation function that switches (SW) the two halves of the data.
4. Function ($\mathrm{f_k}$) again.
5. Permutation function (IP^{-1}): that is the inverse of the initial permutation.

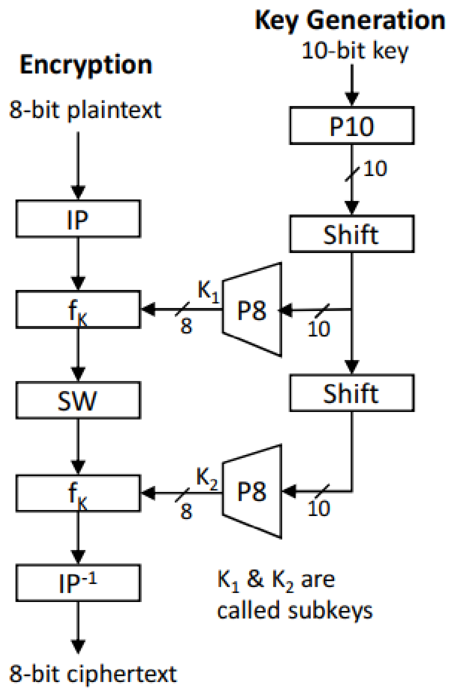


Encryption

- The function f_k has two inputs: data passing through the encryption algorithm and 8-bit key.
- The algorithm could have been designed to work with a 16-bit key, consisting of two 8-bit subkeys, one used for each occurrence of f_k .
- Alternatively, a single 8-bit key could have been used, with the same key used twice in the algorithm.
- A compromise is to use a 10-bit key from which two 8-bit subkeys are generated.
- **In this case:**
  - The key is first subjected to a permutation (P10).
  - Then a shift operation is performed.
  - The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (k_1).
  - The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey (k_2).



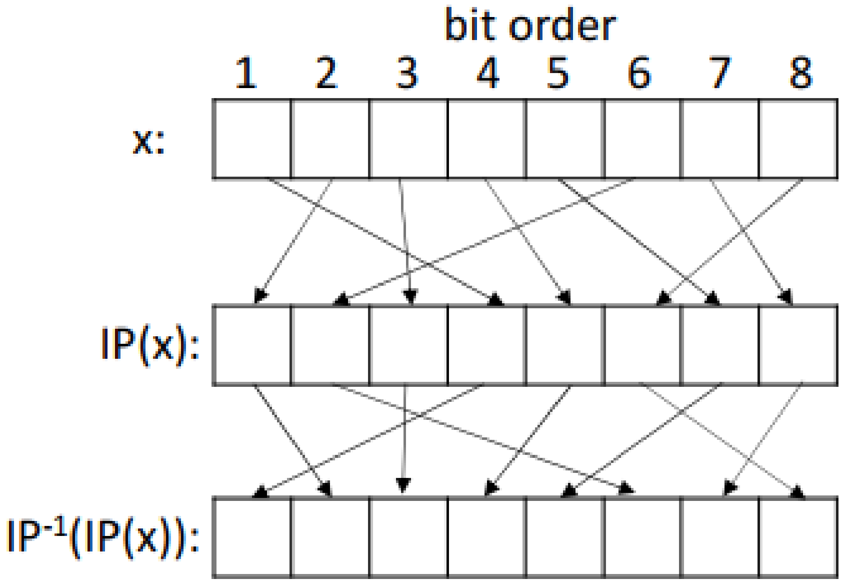
IP (Initial Permutation)



- The 8-bit input plaintext is permuted using the initial permutation function (IP).
- All bits are retained, but re-ordered (mixed).
- At the end of the algorithm, the inverse permutation (IP^{-1}) is used, such that: $IP^{-1}(IP(x)) = x$

e.g., IP = [2 6 3 1 4 8 5 7]

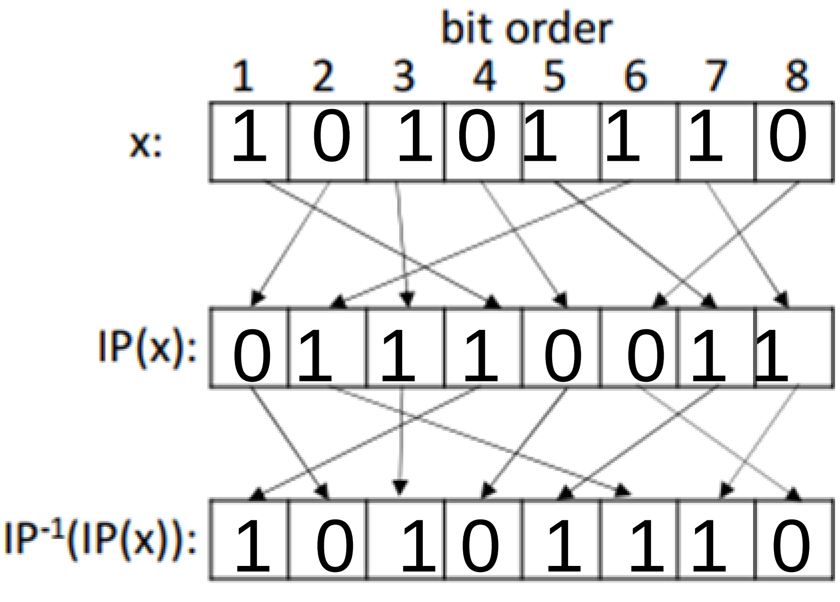
$\therefore IP^{-1}$ = [4 1 3 5 7 2 8 6]



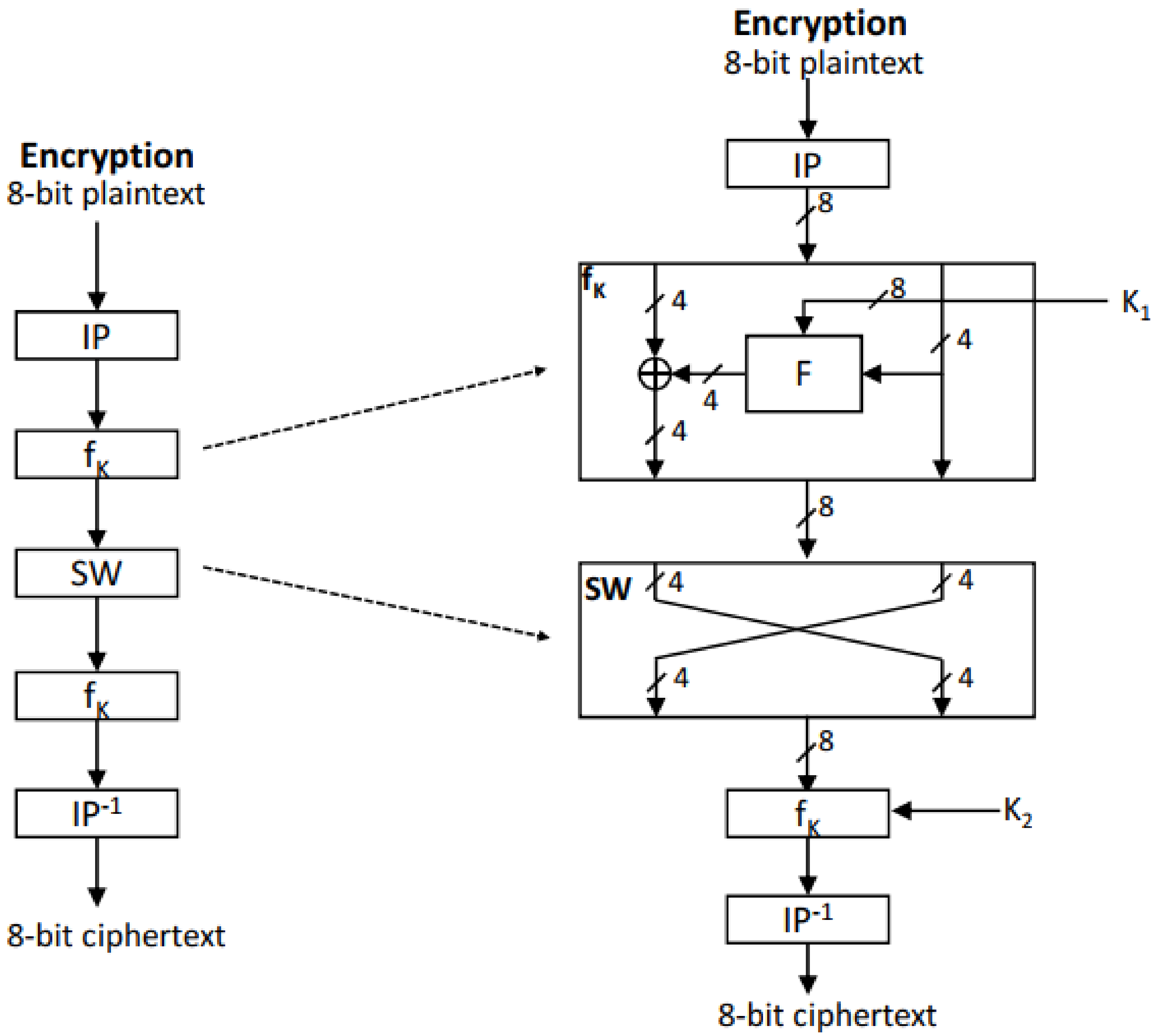
IP (Initial Permutation)

e.g., IP = [2 6 3 1 4 8 5 7]

$\therefore IP^{-1}$ = [4 1 3 5 7 2 8 6]



SW & Function f_k



Function F

In the block F

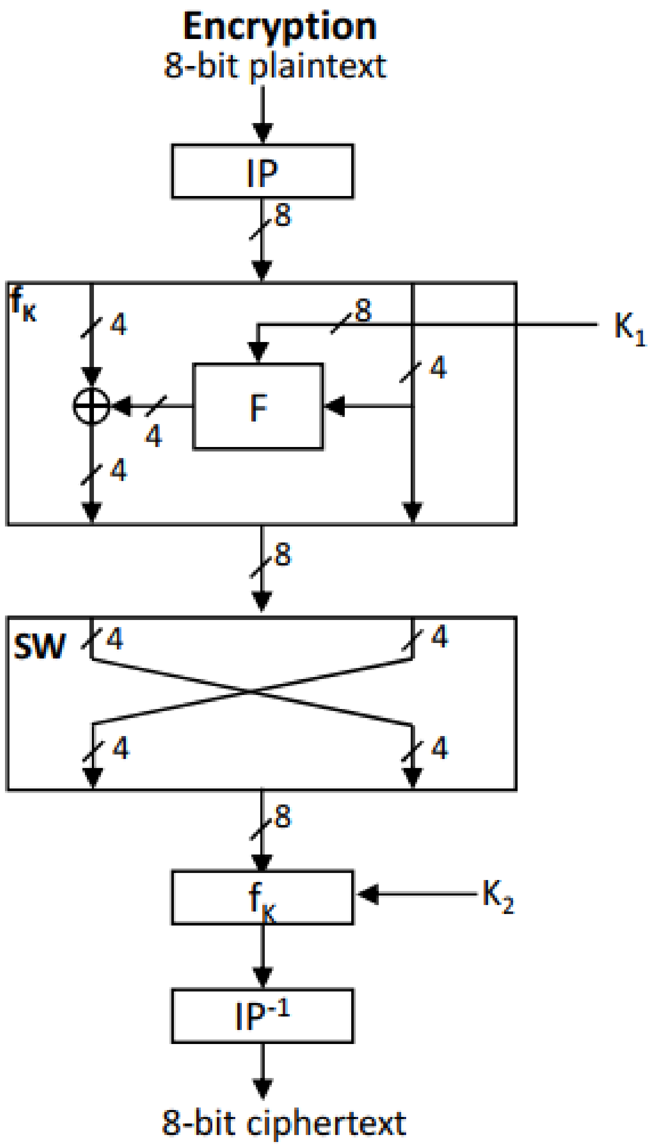
➢ **Ep Box**

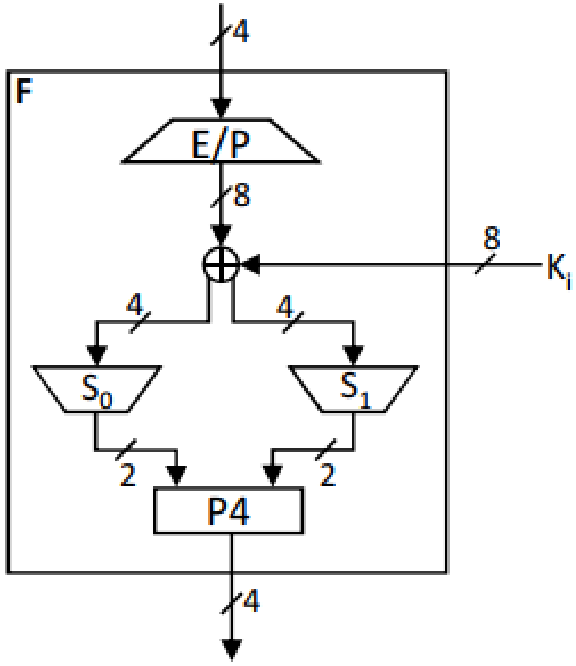
➢ The expansion/permutation (E/P) operation expands the 4 bits into 8 and mixes them.

e.g., E/P = [4 1 2 3 2 3 4 1]

Ex, 1101

11101011





Function F

➢ Substitution Box (S-Box)

- In the block F, two S-boxes (S_0 and S_1) are defined.
- An S-box has a 4-bit input and 2-bit output.
- It operates as follows:

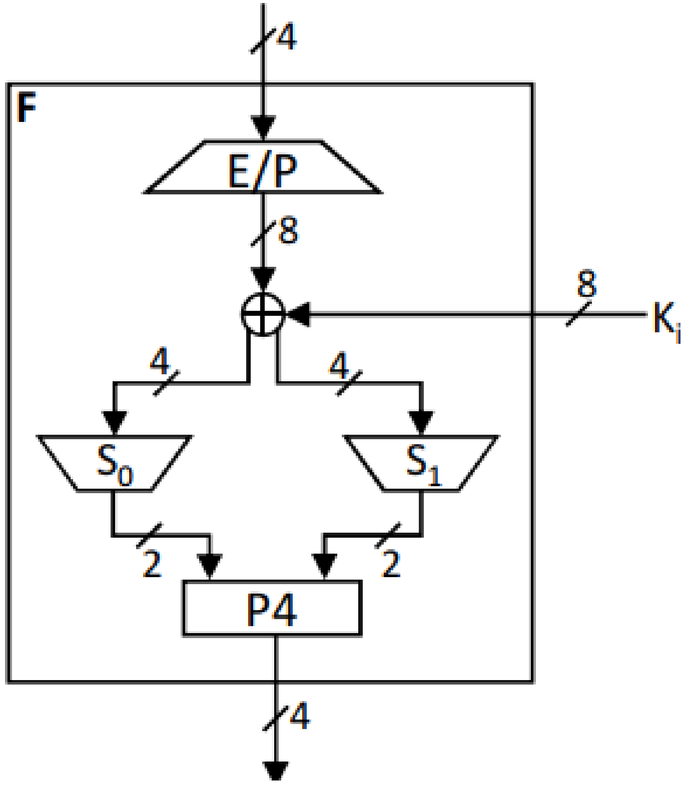
e.g., assume $S_0 = \begin{array}{c c} & \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$, with input 0100

∵ the 1st and 4th bits of the input = 00 = 0

∵ the 2nd and 3rd bits of the input = 10 = 2

∴ the output is selected from row 0 and column 2

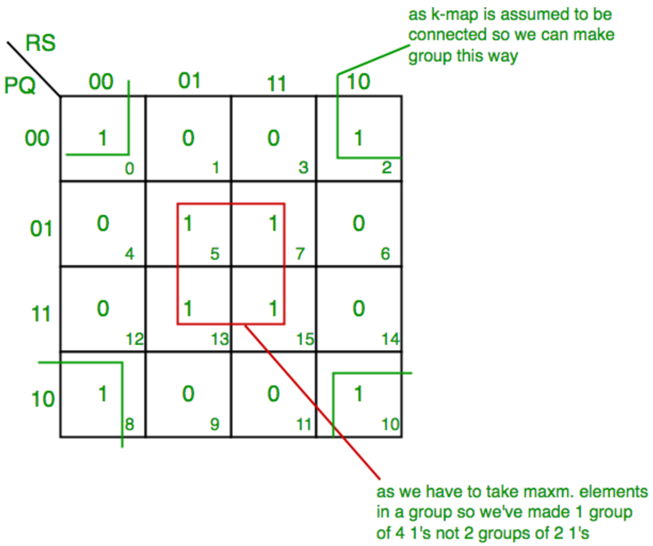
∴ the output = 3 = 11

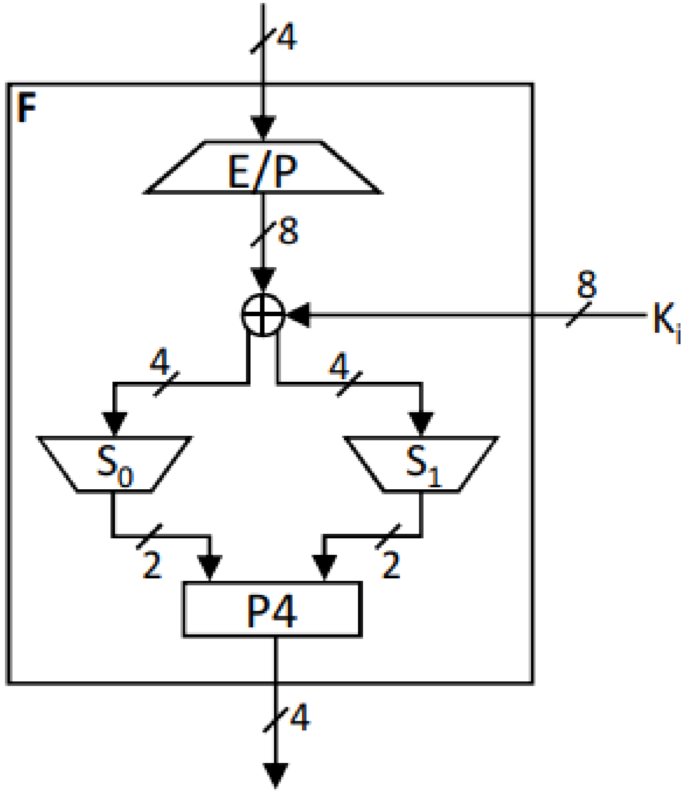


	--00	--01	--10	--11
00--	0011	0000	1011	0101
01--	1000	0100	0111	0010
10--	1111	1100	0110	1110
11--	1001	0001	1010	1101

Design of S-Box

$$S_0 = \begin{array}{c c} & \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$$





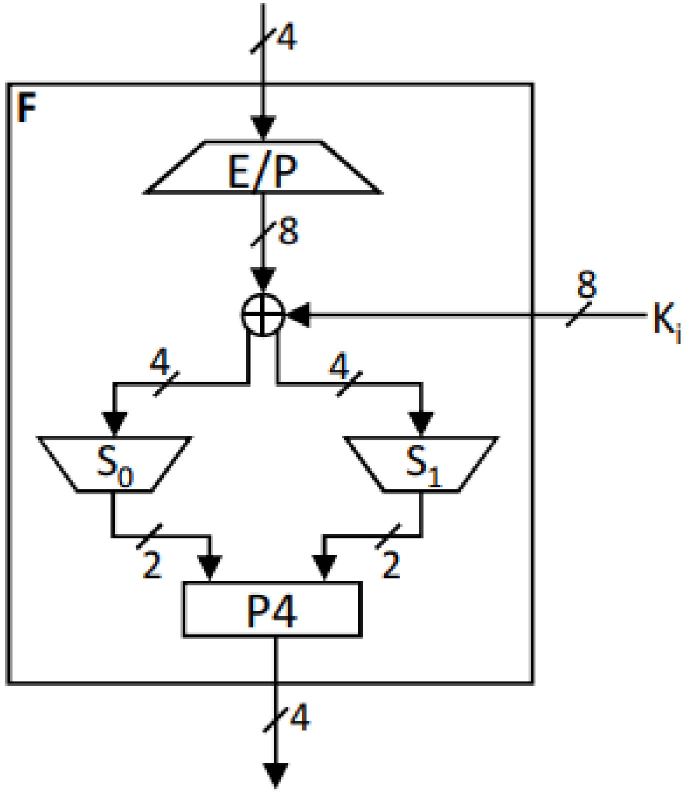
1. Truth Table
2. Karnaugh map
3. Y0 and Y1 equation
4. Logic gate circuit

Function F

- **P4**

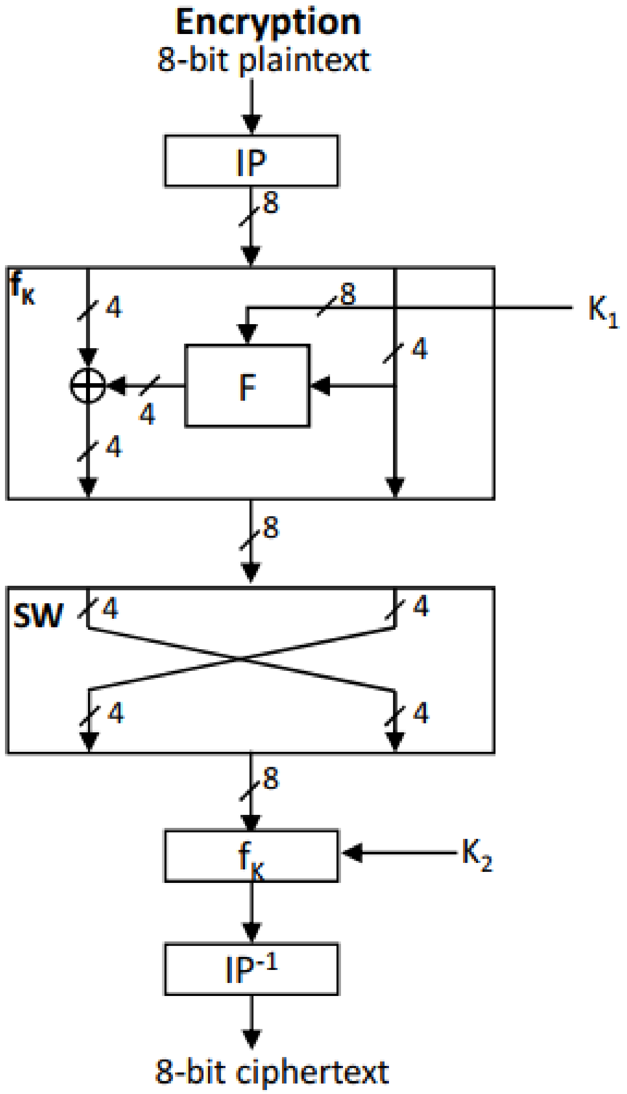
mixes and retains all 4 bits.
P4 [2431]

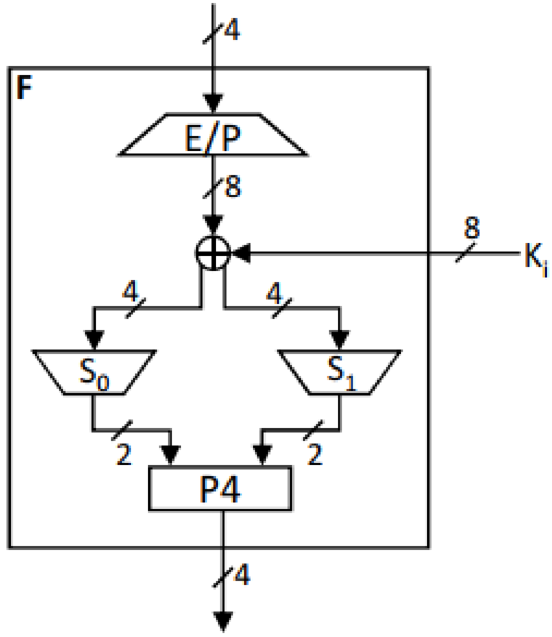
Ex : 0100
1000



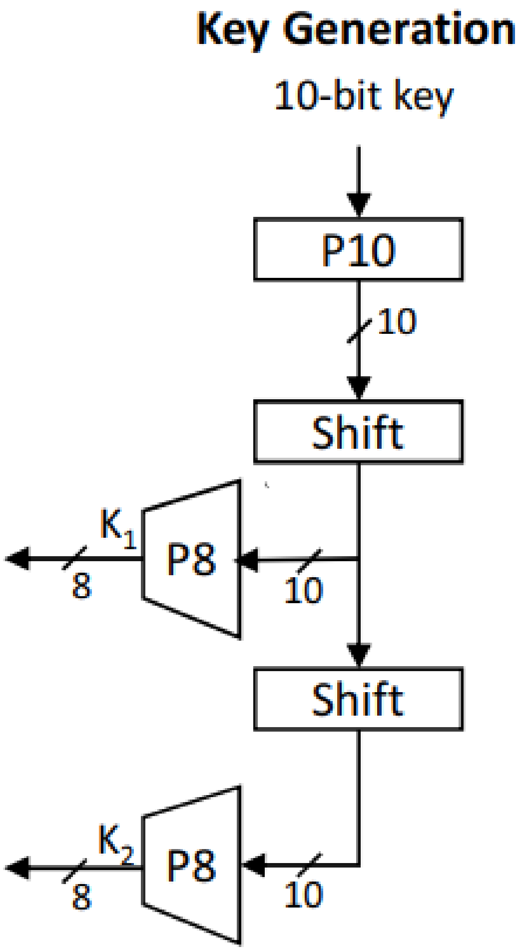
SW & Function f_k

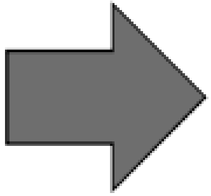
- Only the leftmost 4 bits of the input is altered by the function f_K.
- SW interchanges the left and right 4 bits so that the second round of f_K operates on a different 4 bits.
- In this second round, the E/P, S_0, S_1, and P4 functions are the same. The key input is K_2.

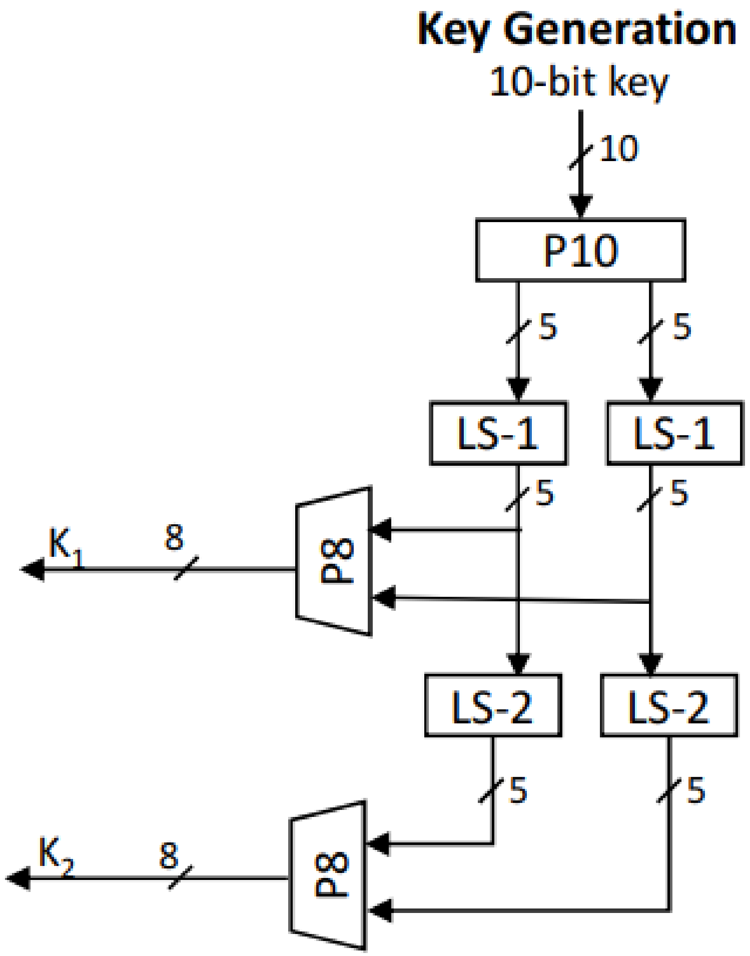




Key Generation







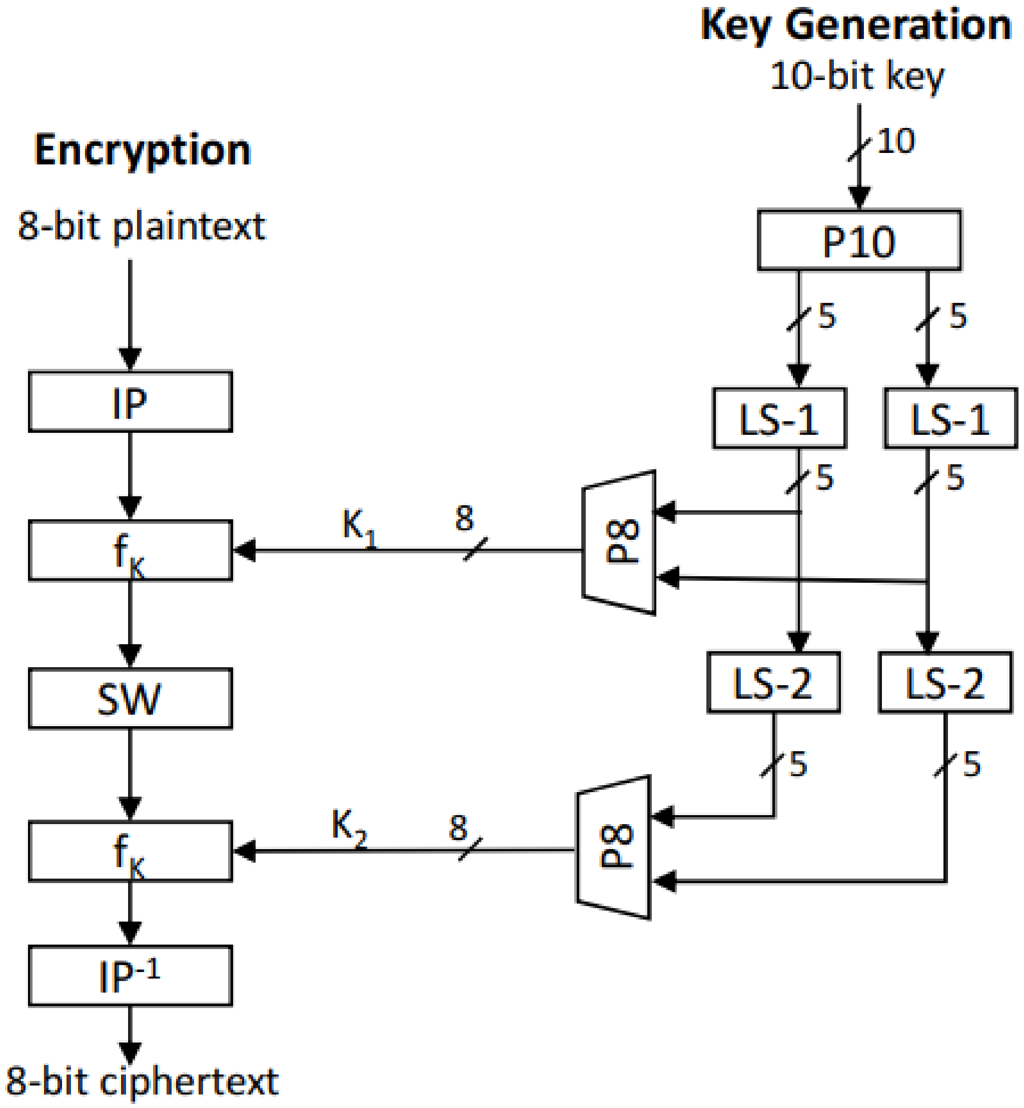
Key Generation

- Key generation includes its own permutation functions; P8 and P10.
- P10 mixes and retains all 10 bits.
- P8 mixes and selects 8 bits out of 10.

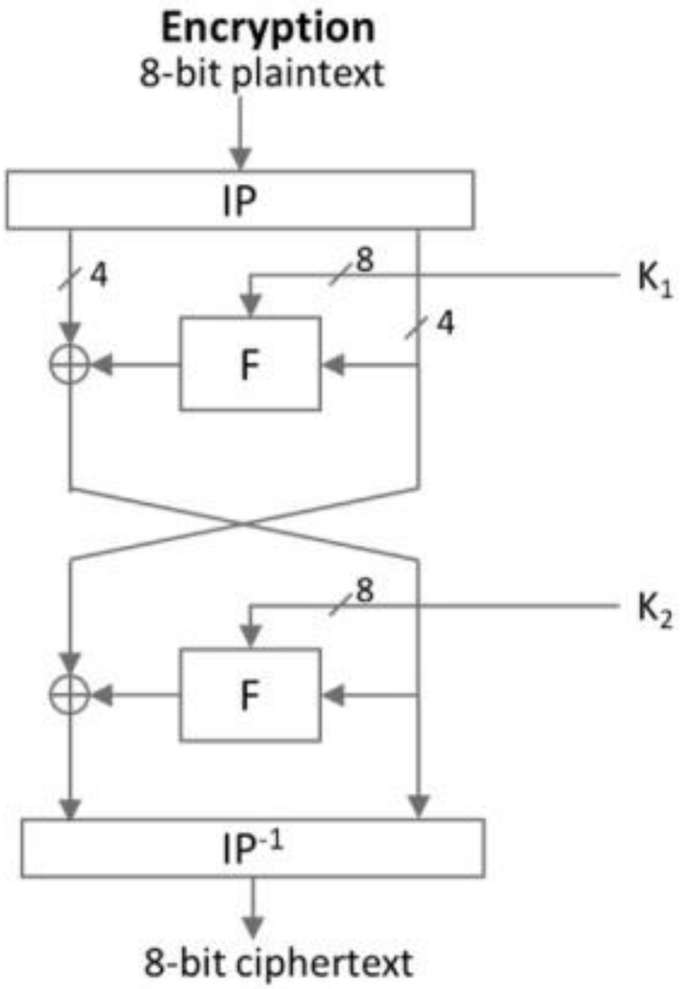
  e.g., P8 = [6 3 7 4 8 5 10 9] . . . bits 1 and 2 are gone..
- LS-1 rotates the input 5 bits one step to the left.

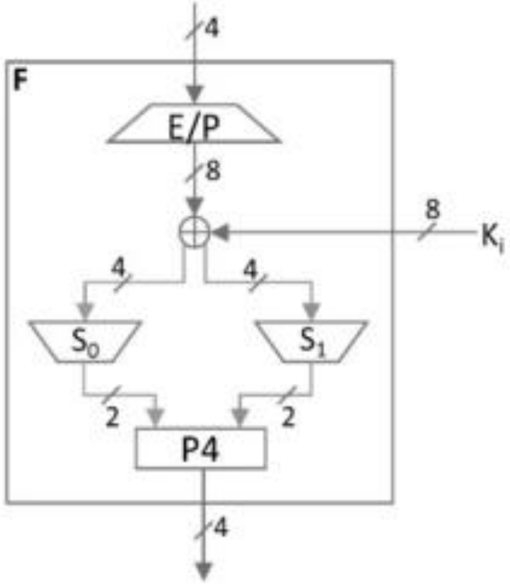
01101 >>> Left shift cycling 11010

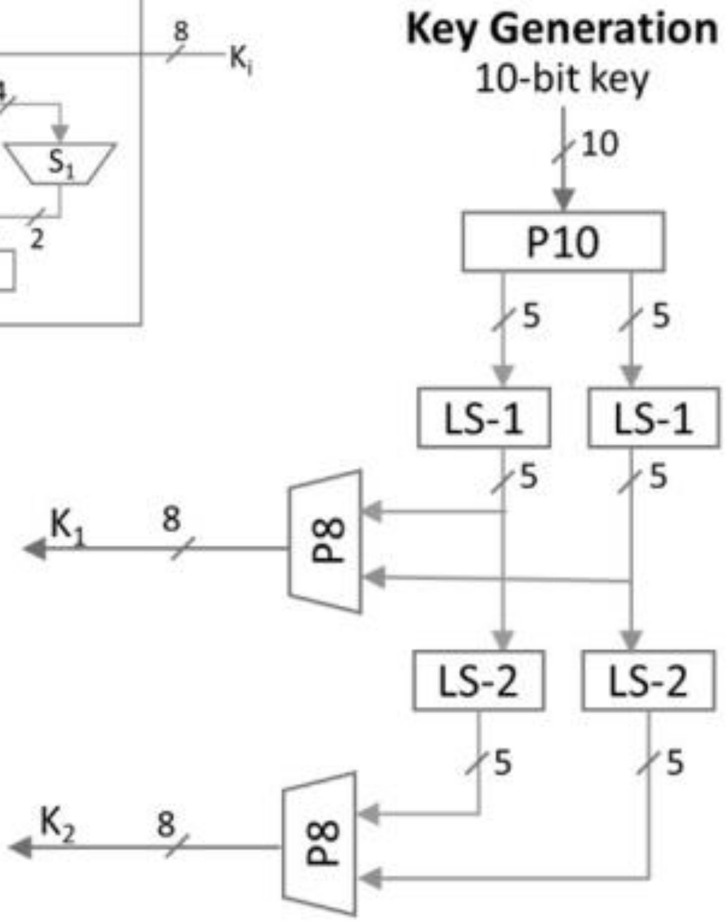
- LS-2 rotates the input 5 bits two steps to the left.



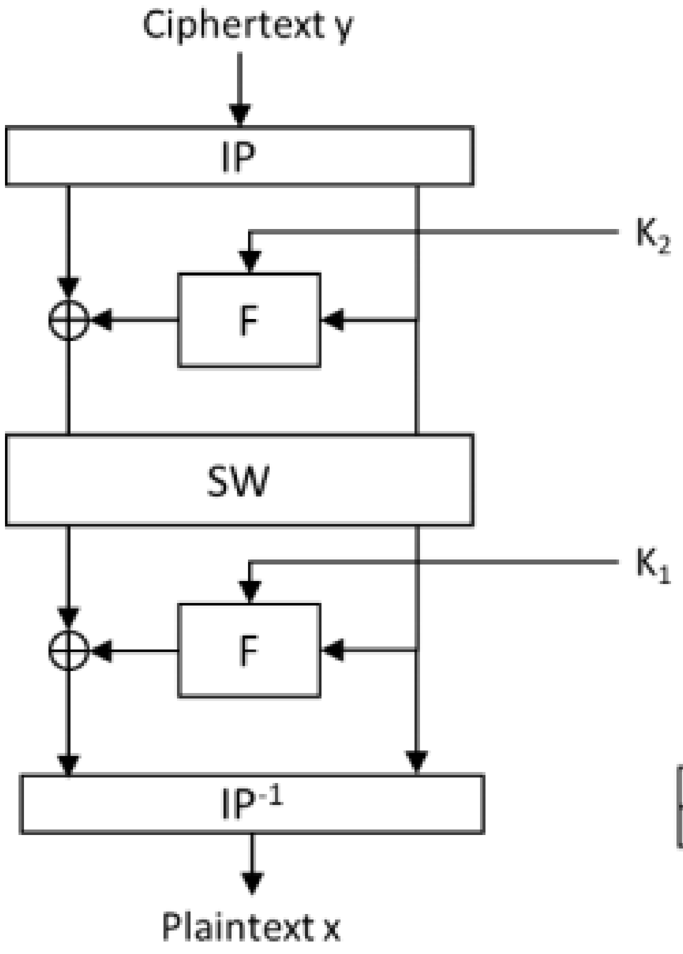
The Whole Picture (Encryption)



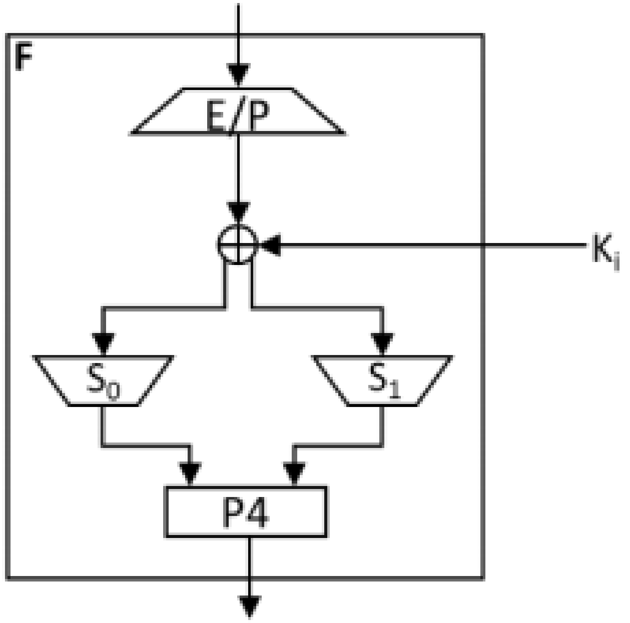




Decryption



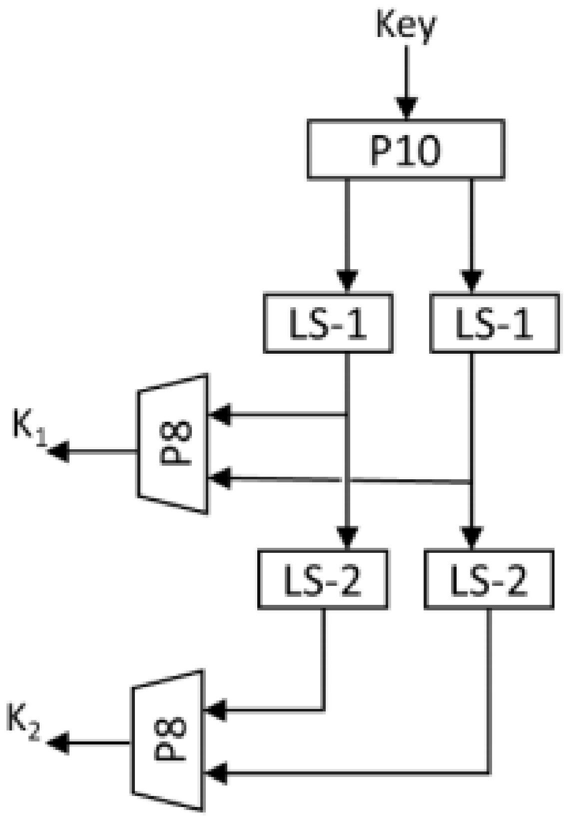
IP							
2	6	3	1	4	8	5	7



P4			
2	4	3	1

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9



E/P							
4	1	2	3	2	3	4	1

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

Security of SDES

- A brute-force attack on SDES is doable.
- With a 10-bit key, there are only 2^{10} = 1024 possibilities.

Relation between DES and SDES

	SDES	DES
Block size	8 bits	64 bits
Key size	10 bits	56 bits
Sub key size	8 bits	48 bit
Function F	Acts on 4 bits	Acts on 32 bits
S-boxes	2	8
S-box size	4 x 4	4 x 16
rounds	2	16

Example

Let the plaintext be the string 0010 1000. Let the 10 bit key be 1100011110

Example

Let the plaintext be the string 0010 1000. Let the 10 bit key be 1100011110

$k1$ = 1110 1001
$k2$ = 1010 0111

the final result of the encryption is 1000 1010

Thank You!

See You next Lectures!!

Any Question?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt
Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451
Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg