Data Encryption Standard (DES)

Dr. Odelu Vanga

IIIT Sri City

Block Ciphers

A block of plaintext is treated as whole text and used to produce a cipher block of equal length

Advantages:

- Fast encryption of large amount of data
- Secrecy and authentication service

Stream Ciphers – encrypts data unit by unit, where a unit is of certain number of bits

Example:

- If the unit be a bit, a stream cipher encrypts data unit by unit. Or
- if the unit be a byte, it encrypts byte by byte

Vigenere Cipher

Diffusion & Confusion :

CLAUDE SHANNON in 1945:

"Introduce diffusion and confusion through cryptographic algorithms"

DIFFUSION:

- Use permutation followed by some functional transformation.
- Make statistical relationship between the plaintext and ciphertext as complex as possible.

CONFUSION:

- Makes the relationship between the statistics of ciphertext and encryption key as complex as possible.
- Achieved by using a complex substitution algorithm.

Substitution or Permutation: easy to break by using statistical analysis;

Strength due to non-linear functional transformation.

Kerckhoff's Rule

The strength of an encryption algorithm depends upon:

1. Design of the algorithm
2. Key length
3. Secrecy of the key
   (requires proper management of key distribution)

Cryptosystems should rely on the secrecy of the key, but not of algorithm

Modern Encryption Techniques:

- DES: A complex encryption scheme.
- Simplified DES:
  - A teaching tool
  - Designed by Prof. Edward Schaeter, Santa Clara University, 1996

Given: plaintext 8-bit, Key 10-bit

Output: ciphertext 8-bit

Simplified DES:

$$\text{ciphertext} = IP^{-1}(f_{k2}(SW(f_{k1}(IP(\text{plaintext})))))$$

S-DES's five steps:

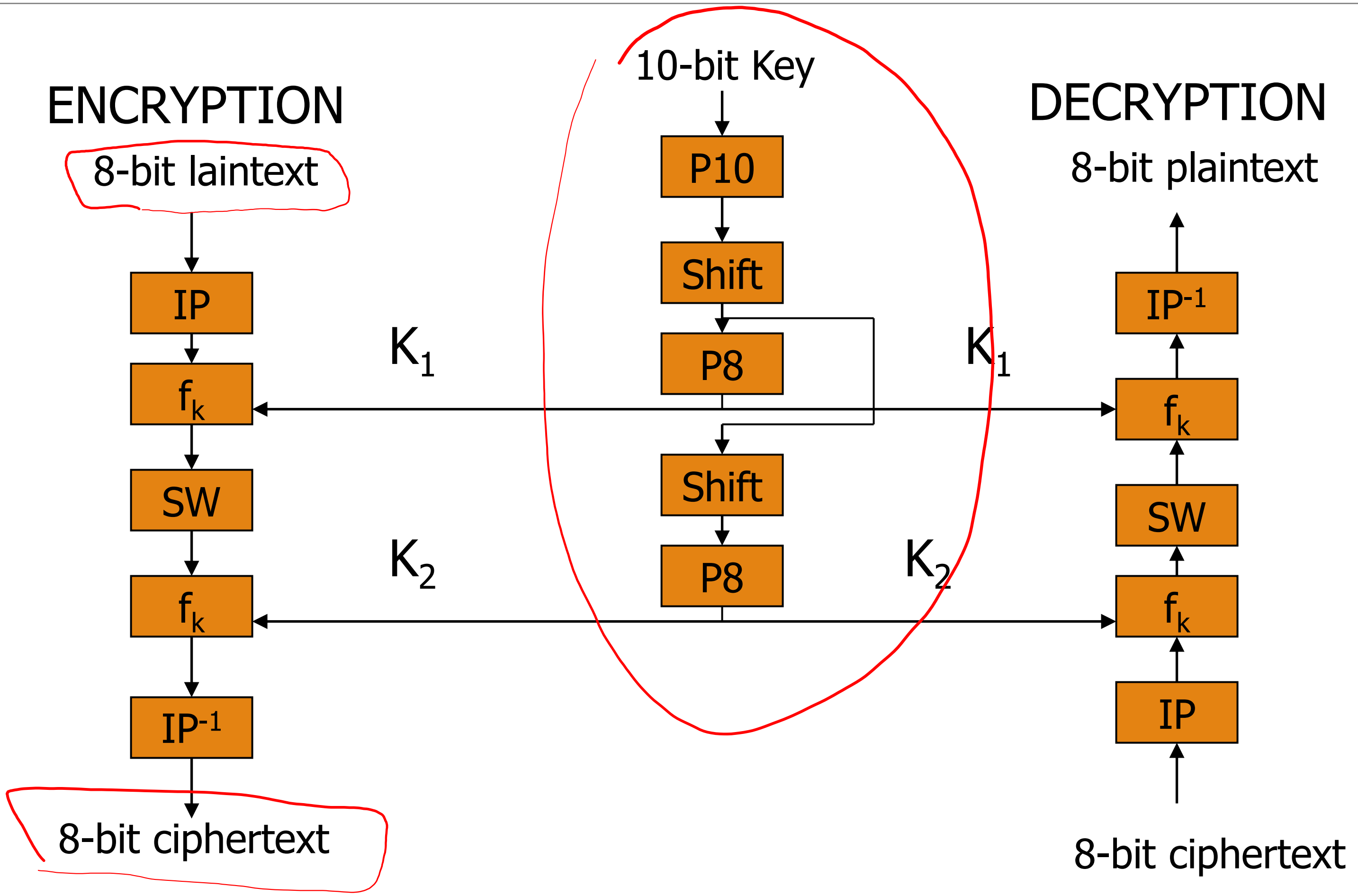
1. Initial Permutation **IP**.
2. A complex function $\mathbf{f_k}$ which requires key $\mathbf{K_1}$.
3. A switch function **SW**
   - switches the left half and the right half of a data string.
4. The function $\mathbf{f_k}$ again with a different key $\mathbf{K_2}$.
5. A permutation function that is the **inverse of IP** –called $\mathbf{IP^{-1}}$.

   Then we have $\mathbf{(IP^{-1}(IP(X))) = X}$

S-DES may be said to have two ROUNDS of the function $\mathbf{f_k}$.

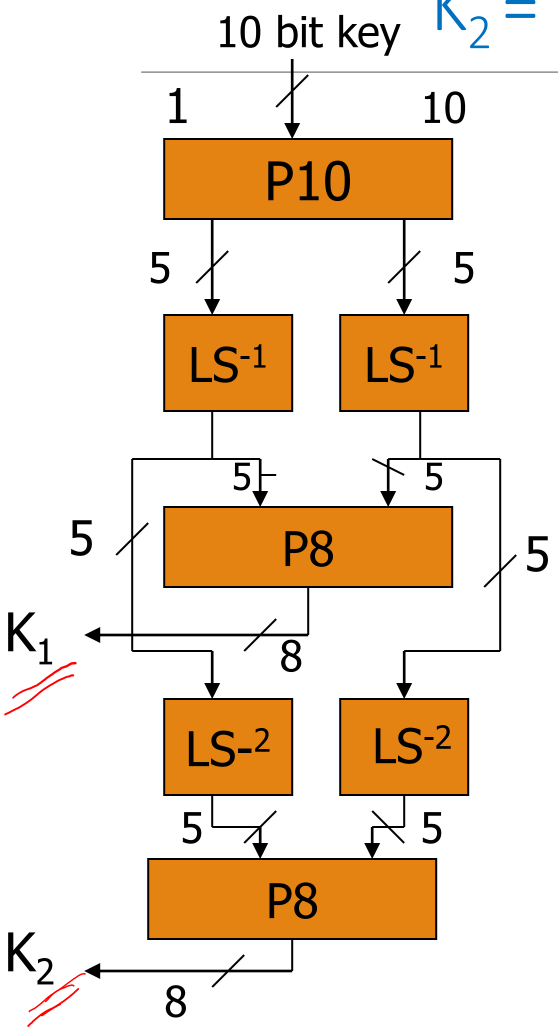
Simplified DES scheme:

$$\text{ciphertext} = IP^{-1}(f_{k2}(SW(f_{k1}(IP(\text{plaintext})))))$$
$$\text{Plaintext} = IP^{-1}(f_{k1}(SW(f_{k2}(IP(\text{ciphertext})))))$$



Key generation for simplified DES:

$$K_1 = P8\,(\,Shift\,(P10\,(Key)))$$
$$K_2 = P8\,(\,Shift\,(\,Shift\,(P10\,(Key))))$$



P10

3	5	2	7	4	10	1	9	8	6

Circular left shift by 1, separately on the left and the right halves

P8

6	3	7	4	8	5	10	9

Circular left shift by 2 , separately on the left and the right halves

P8

6	3	7	4	8	5	10	9

P10 | 3 5 2 7 4 10 1 9 8 6

P8 | 6 3 7 4 8 5 10 9

$K_2 = P8(\text{Shift}^2(P10(K)))$

K_1:

Bit #	1	2	3	4	5	6	7	8	9	10
K	1	1	0	0	0	1	1	1	1	0
P10(K)	0	0	1	1	0	0	1	1	1	1
Shift(P10(K))	0	1	1	0	0	1	1	1	1	0
P8(Shift(P10(K)))	1	1	1	0	1	0	0	1		

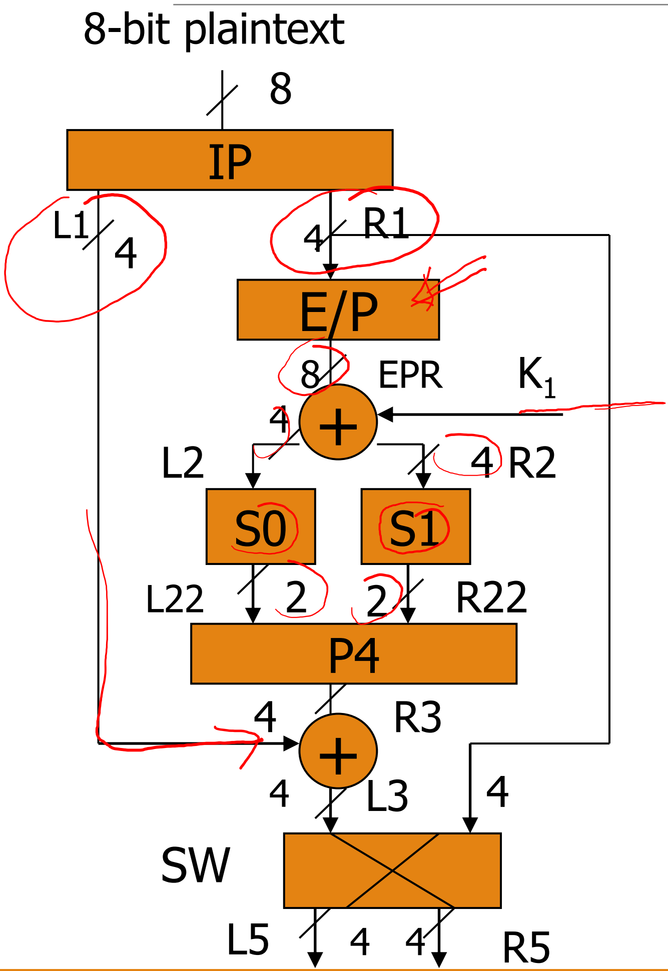
11000 | 11101

$K_1 = 11101001$

$K_2 = \boxed{10101010}$

Simplified DES Encryption:

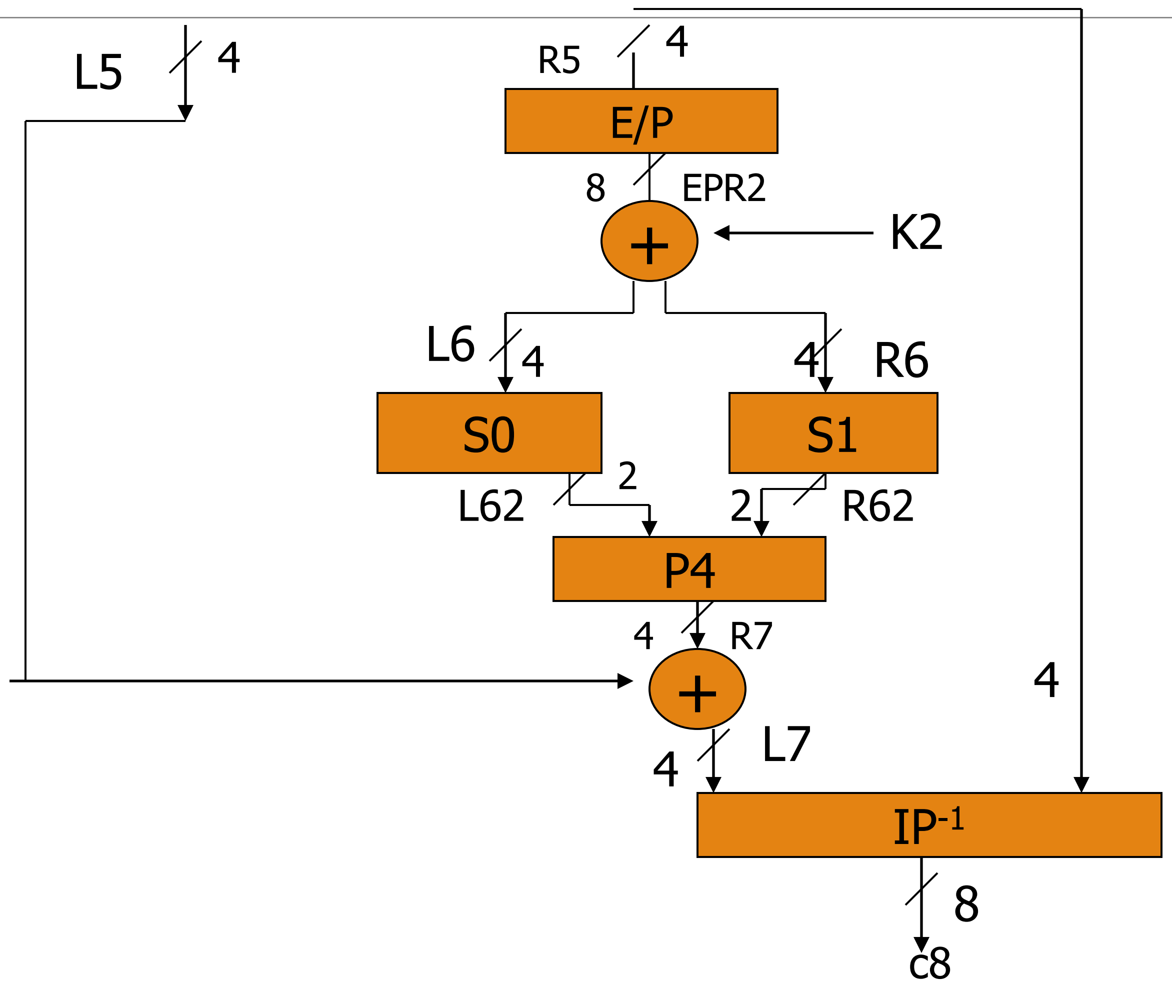
$$ciphertext = IP^{-1}(f_{k2}(SW(f_{k1}(IP(plaintext)))))$$



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

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

2	4	3	1	P4



L5
4
R5
4
E/P
8
EPR2
K2
L6
4
4
R6
S0
S1
2
L62
2
R62
P4
4
R7
4
L7
4
IP-1
8
c8

Inverse of a permutation

2	6	3	1	4	8	5	7

$f : X \to Y$ bijective

$f^{-1} : Y \to X$

$f : X \to X$ bijective.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \boxed{2} & 6 & \boxed{3} & \boxed{1} & 4 & 8 & 5 & 7 \end{pmatrix}$$

$(f \circ g)(x)$

$f(1) = 2$ $f(5) = 4$

$f(2) = 6$ $f(6) = 8$

$f(3) = 3$ $f(7) = 5$

$f(4) = 1$ $f(8) = 7$

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 5 & 7 & 2 & 8 & 6 \end{pmatrix}$$

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

$\boxed{f(x) = x}$

$f^{-1}(1) = 4$

$f(f^{-1}(1)) = f(4) = 1$

plaintext: 0010 1000

K_1 : 1110 1001

K_2 : 1010 1010

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

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

Bit #	1	2	3	4	5	6	7	8
P	0	0	1	0	1	0	0	0
IP(P)	0	0	1	0	0	0	1	0

$P = (L, R)$

$F(p, k) \to$ 4-bit

p: 4 bit, k: 8 bit

P4 : 2 4 3 1

E/P : 4 1 2 3 2 3 4 1

$$f_k(L, R) = (L \oplus F(R, SK), R)$$

$$SW(L, R) \to (R, L)$$

$$IP^{-1} \circ f_{k_2} \circ SW \circ f_{k_1} \circ IP$$

E/P : Expansion permutation.

Input: $n_1 n_2 n_3 n_4$ (4-bit)

$$\begin{array}{c|cc|c} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{array}$$

$$\begin{array}{cccc} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{array}$$

$$\begin{array}{c|cccc|c} n_{32} & n_1 & n_2 & n_3 & n_4 & n_5 \\ n_4 & n_5 & n_6 & n_7 & n_8 & n_9 \\ \vdots & n_9 & n_{10} & \cdots & & \vdots \\ & \vdots & & & & \vdots \\ n_{28} & n_{29} & n_{30} & n_{31} & n_{32} & n_1 \end{array}$$

$IP(P) = 0010\ 0010$

E/P : $\boxed{4\ 1\ 2\ 3\ 2\ 3\ 4\ 1}$

P4 : $\boxed{2\ 4\ 3\ 1}$

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array}$$

$$S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & \boxed{0} & 3 \end{array}$$

Bit #	1	2	3	4	5	6	7	8
R	0	0	1	0				
E/P (R)	0	0	0	1	0	1	0	0
K_1	1	1	1	0	1	0	0	1
E/P(R) ⊕ K_1	1	1	1	1	1	1	0	1
SBox(E/P(R) ⊕ K_1)	1	0	0	0				
P4(SBox(E/P(R)+K_1))	0	0	0	1				

column

1 11 1 — S0

1 10 1 — S1

row.

S0 : (11, 11) = (3, 3)

S1 : (11, 10) = (3, 2)

final cipher :

1010 1110 ??

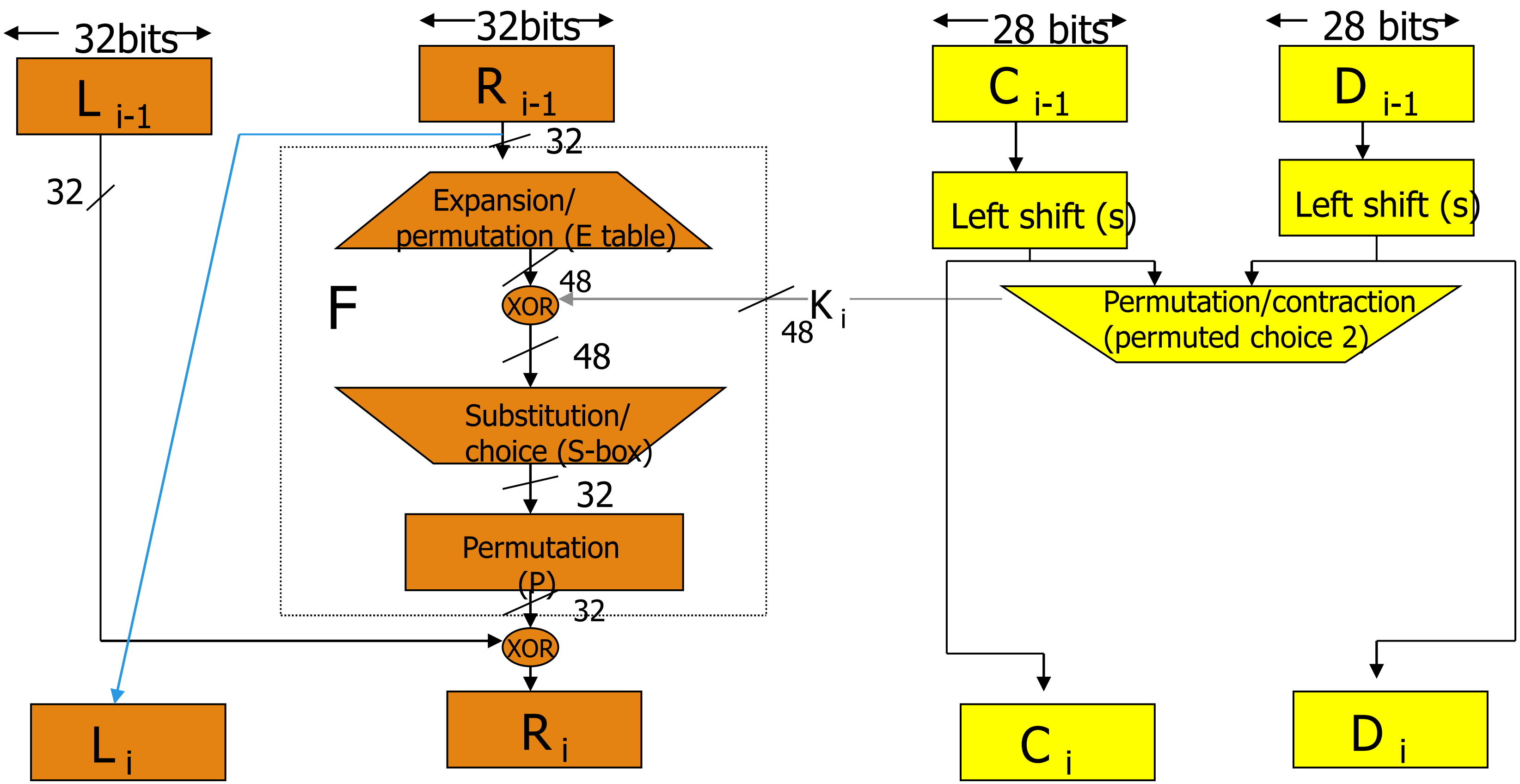
DES Encryption:

DES: a public standard. But its design criterion has not been published. 64-bit block and 56-bit key

64 bit plaintext goes through

- an Initial Permutation (IP).
- 16 Rounds of a complex function f_k as follows:
  - Round 1 of a complex function f_k with sub key K_1 .
  - Round 2 of a complex function f_k with sub key $K_{2.}$
  - Round 16 of a complex function f_k with sub key K_{16}
- **At the end of 16 rounds, the Left-half and Right-half are swapped.**
- an Inverse Initial Permutation (IP^{-1}) **to produce 64 bit ciphertext**.

Fig : single Round of DES Algorithm:



i-th Round

The part in yellow, in the previous slide, shows the sub key generation. After PC1, the circular rotations are independent for the left half and the right-half.

ENCRYPTION: In the i-th round,

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, Ki)$$

$$= L_{i-1} \oplus P(S(E(R_{i-1}) \oplus Ki))$$

Where E: expansion from 32 bits to 48

S: Using 8 S-boxes to convert 48 bits to 32 bits – each S box converts 6 bits to 4 bits

P: permutation

Thank You