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 $\mathbf{IP^{-1}}$.

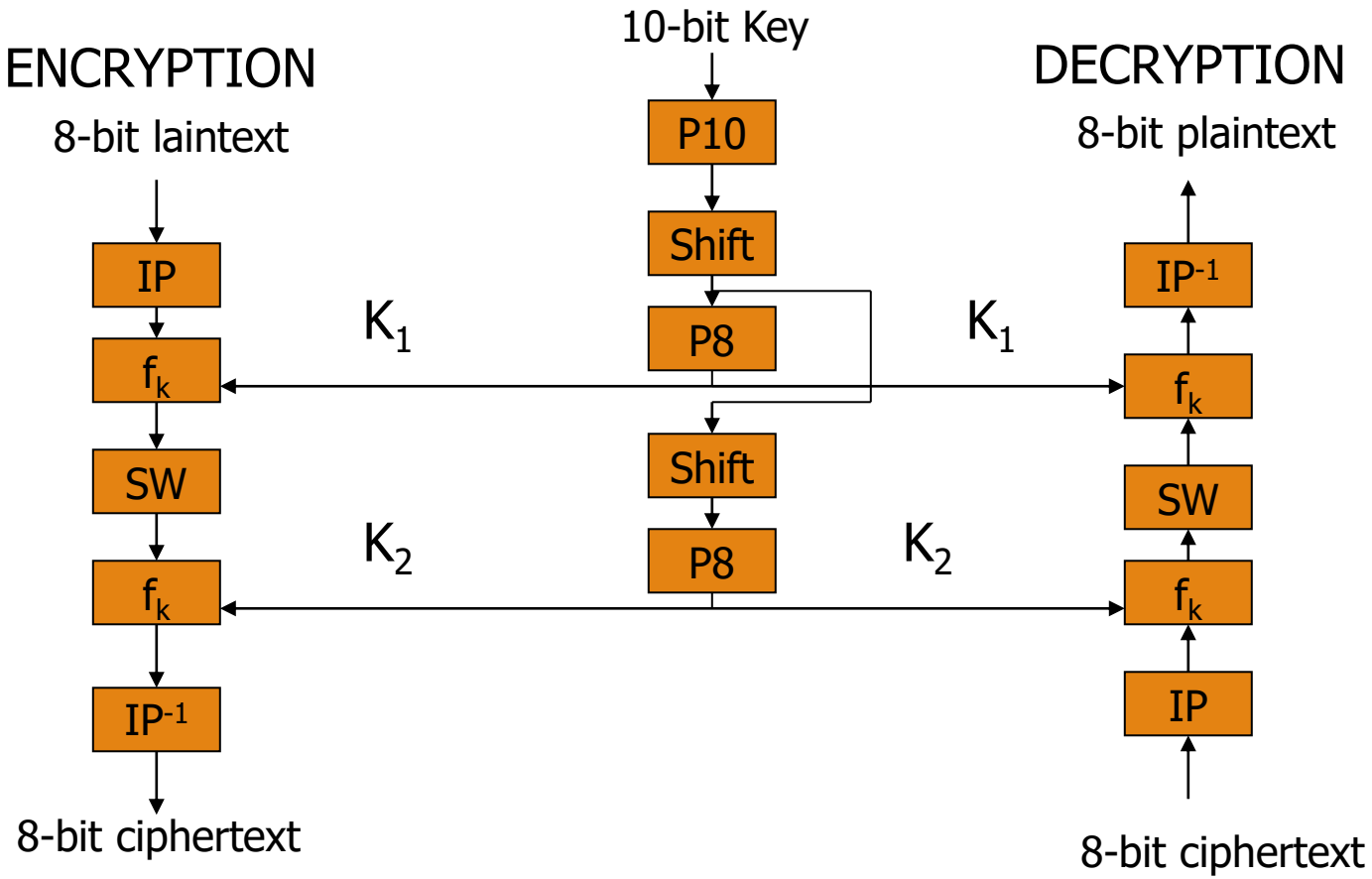
   Then we have $\mathbf{(\ IP^{-1}(\ IP\ (X)\ ))\ = X}$

S-DES may be said to have two ROUNDS of the function f_k.

Simplified DES scheme:

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

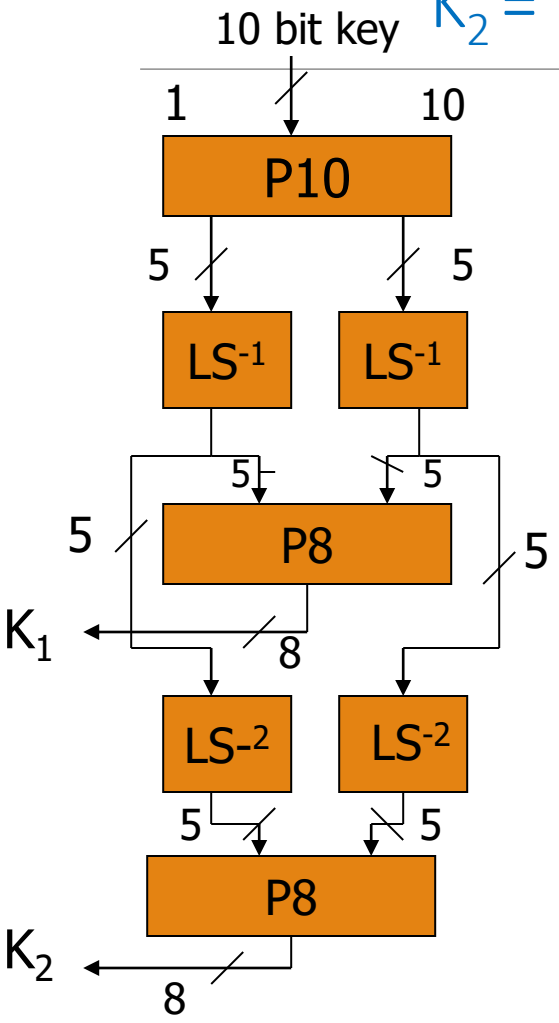
$$Plaintext = IP^{-1}(f_{k1}(SW(f_{k2}(IP(ciphertext)))))$$



Key generation for simplified DES:

K_1 = P8 (Shift (P10 (Key)))

K_2 = P8 (Shift (Shift (P10 (Key))))



3	5	2	7	4	10	1	9	8	6

P10

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

6	3	7	4	8	5	10	9

P8

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

6	3	7	4	8	5	10	9

P8

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

P8 | 6 3 7 4 8 5 10 9

$K_2 = P8(shift^2(P10(K)))$

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		

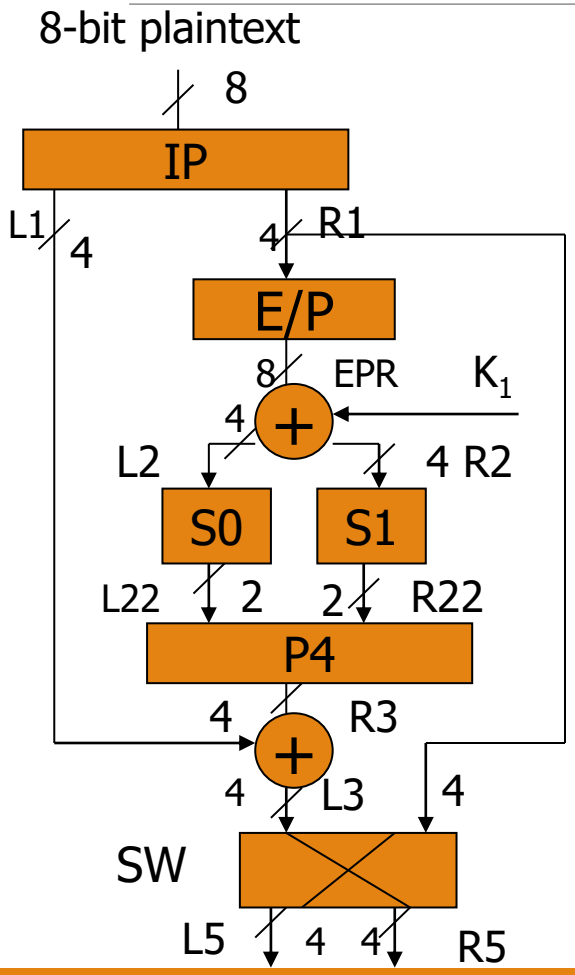
11000 | 11101

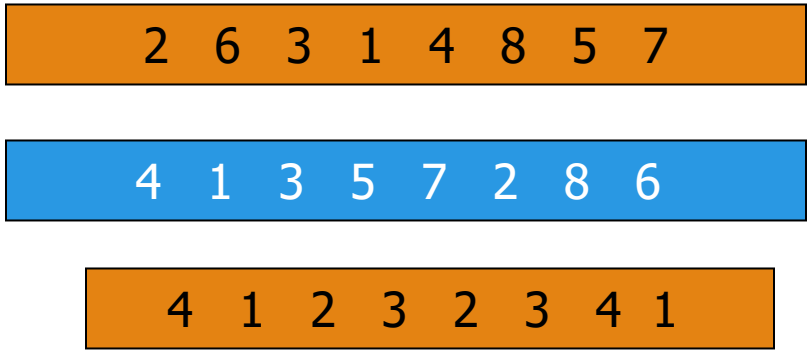
$K_1 = 11101001$

$K_2 = 10101010$

Simplified DES Encryption:

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



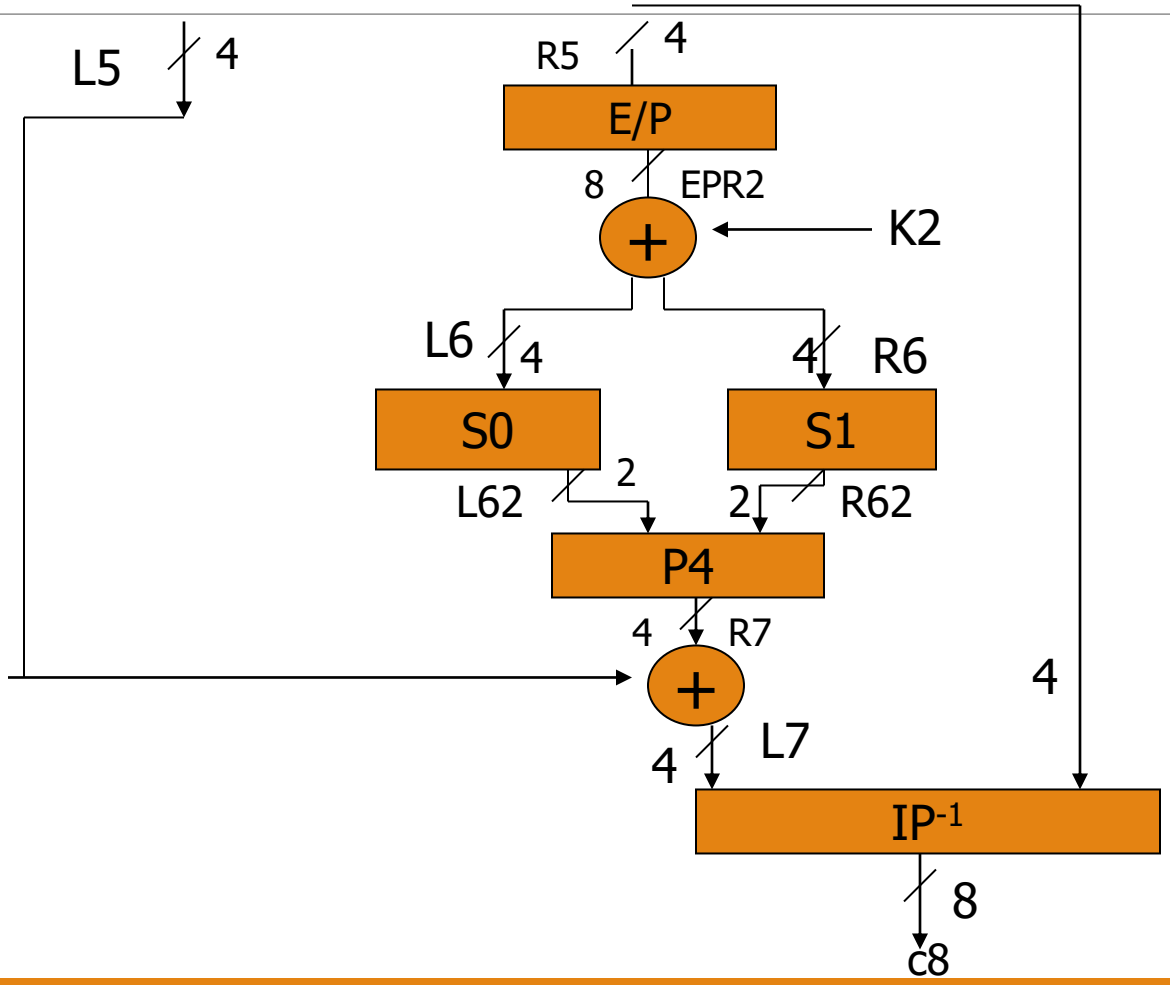


$S0 =$

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

$S1 =$

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3


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