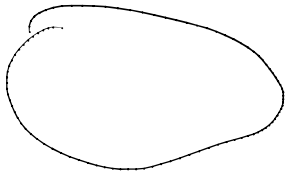
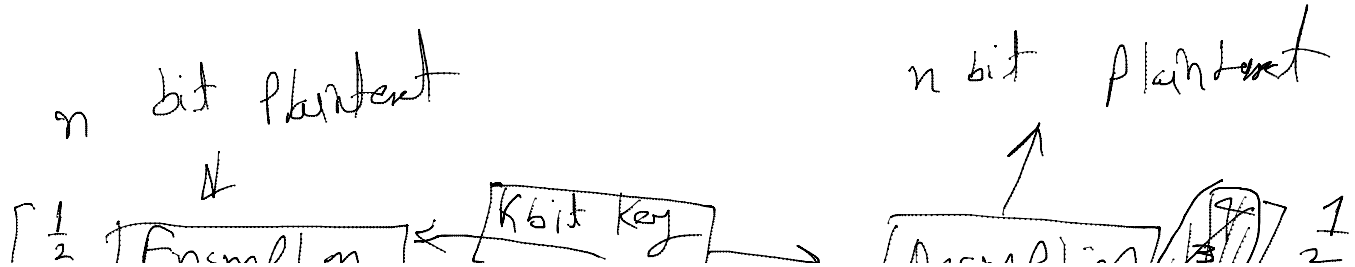
Modern symmetric key cryptography (cipher)

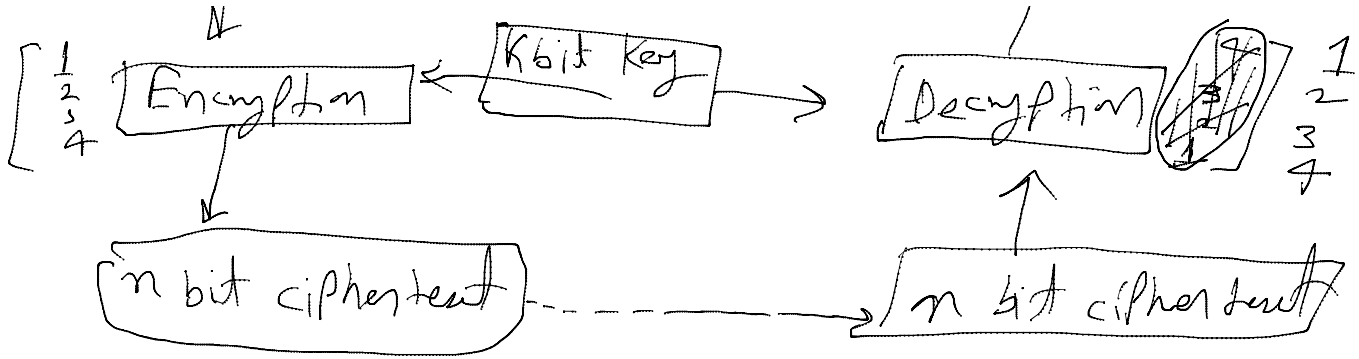


character oriented cipher: only for text based data

bit oriented cipher :=> Increase security

→ Convinient for graphics, audio & video files.





If msg has few bit than n bits (n is block size), padding must be added to make it n-bit block. if msg has more than n bit, it should be devided into the blocks (n bit)

Q. The plaintext msg = 100 char, Block size is 64 bits, Char encoding is 8 bit ASCII. find ① Total No. of Block.
② Padding bits required for last block. 32

Sol: total No. of bits = 800

∵ 1 block size = 64

① Total block = 800

① Total block = 800

=

64

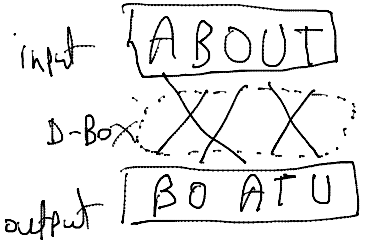
② Padding bits in last block = 800 mod 64 = 32

Padding bit = 64 − 32 = 32

(Block size ↑ , bit in Last Block ↑)

Components of modern Block ciphers:

① D-Boxes: (Diffusion Box) It transpose bits



Transpose :

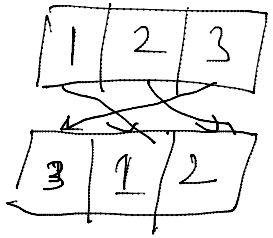
1	2	3	4	5
3	1	2	5	4

Transpose table

D-Box are three types:

D-Box are three types:

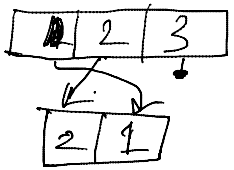
(a) straight D-Box :



input size = 3

output size = 3

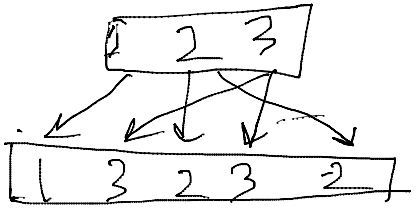
(b) Compression D-Box :



Input size = 3

output size = 2

(c) Expansion D-Box :



input = 3

output = 5

(2) S-Box : (substition Box) :

↓

Replaced by other

n input : $x_1, x_2, x_3 \cdots x_n$

m output : $y_1, y_2, y_3 \cdots y_m$

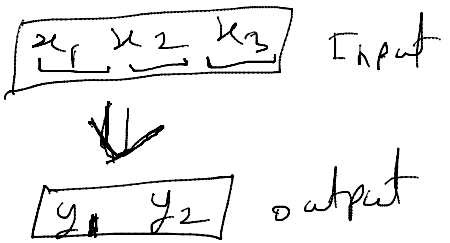
$y_i = f_i(x_1 \cdots x_n)$

(a) Linear S-Box :

(b) Non linear S-Box :

Ex: (1) input $X = \{x_1\ x_2\ x_3\}$

output $Y = \{y_1, y_2\}$



(a) $f_1^n = \{ y_1 = x_1 \oplus x_2 \oplus x_3 \}$

$\{ y_2 = x_1 \}$

(b) $f_1^n = \{ y_1 = x_1 \cdot x_2 \}$

$\{ y_2 = x_1 + x_2 x_3 \}$

$y_3 =$

X

(c)

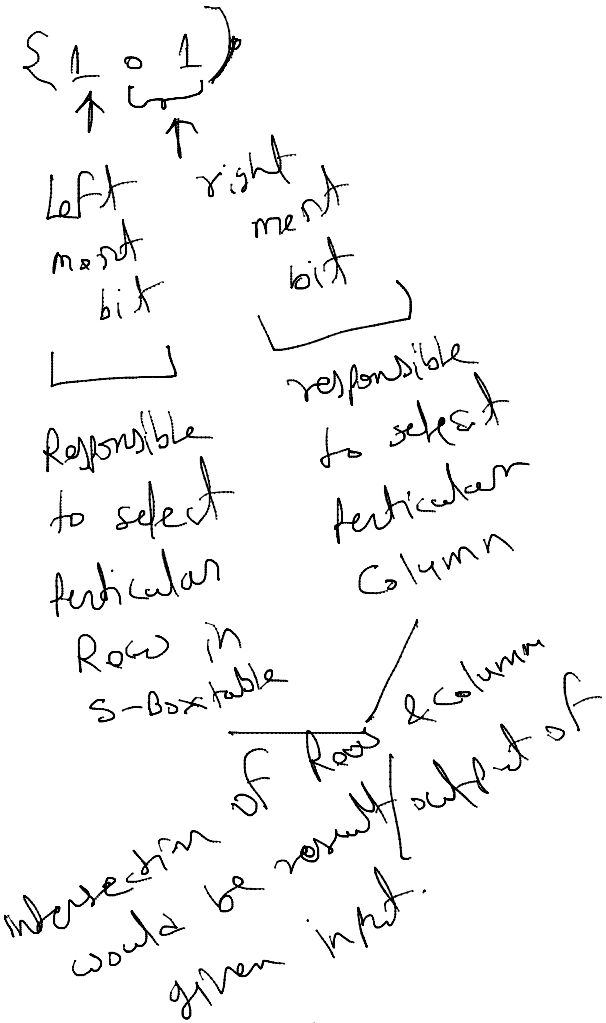
Left most bit ↘ | 00 | 01 | 10 | 11 | ← right most bit

	00	01	10	11
0	00	10	01	11
→ 1	10	00	11	01

S-Box table

Suppose input $\{x_1 x_2 x_3\} = \{1\ 0\ 1\}$

then output = ?



DES (Data Encryption Algorithm):

- Developed by NIST (National Institute of standard technology)
- Symmetric key Block Cipher
- It is implementation of Feistel cipher Model.

- DES has 16 Round.
- Block size is 64 bit. (plaintext & ciphertext)
- Key length is 56 bit. (original key is 64 bit but 8 bit are not used)

0 1 2 3 4 5 6 (7) 8 9 10 11 12 13 14 (15) 16 17 18 19 20 21 22 23

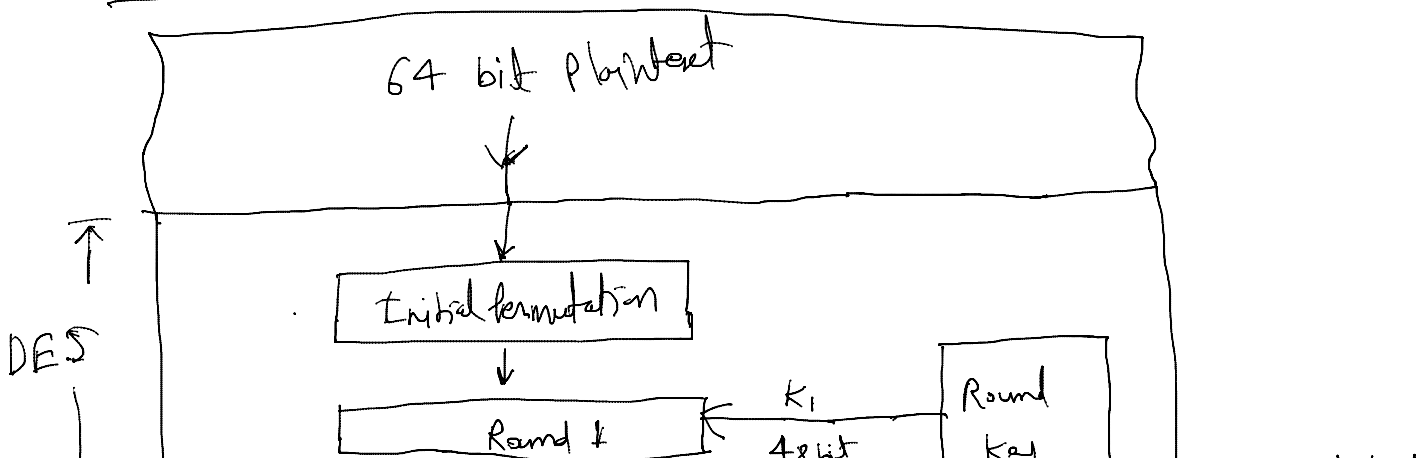
7 bit — 7 bit lost — 7 bit — 7 bit lost

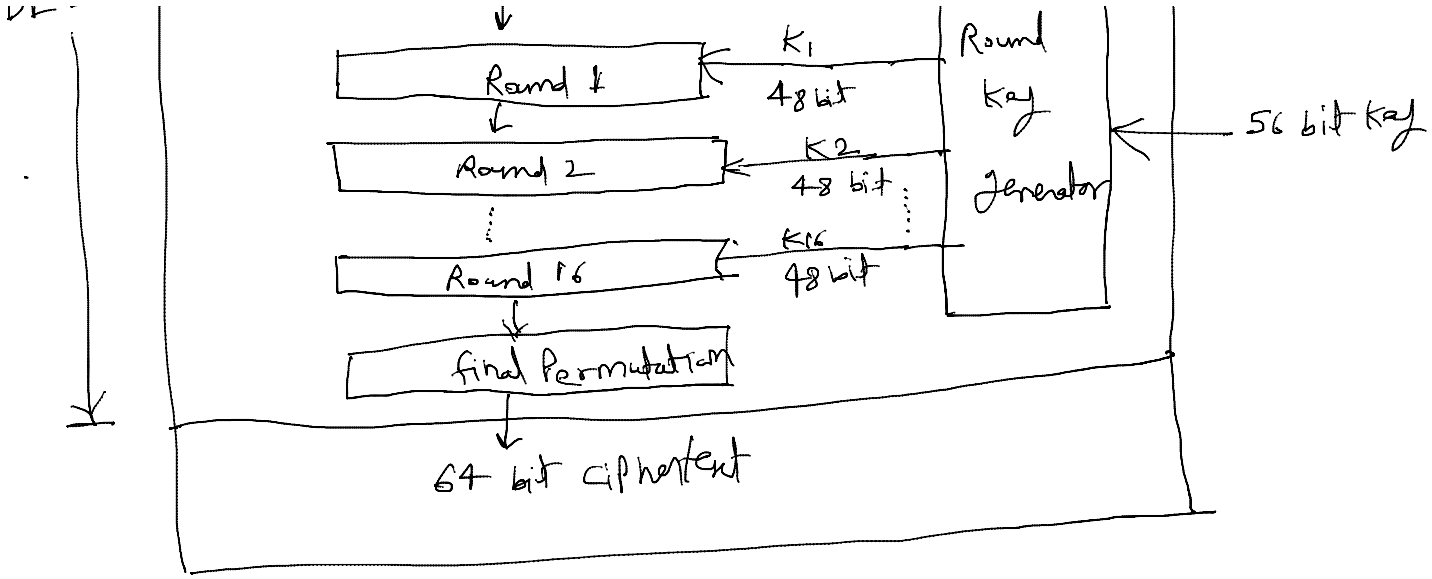
$7 \times 8 = 56$ bit

main functionality of DES:

1. Round function
2. key schedule
3. Additional Processing (Initial & final permutation)

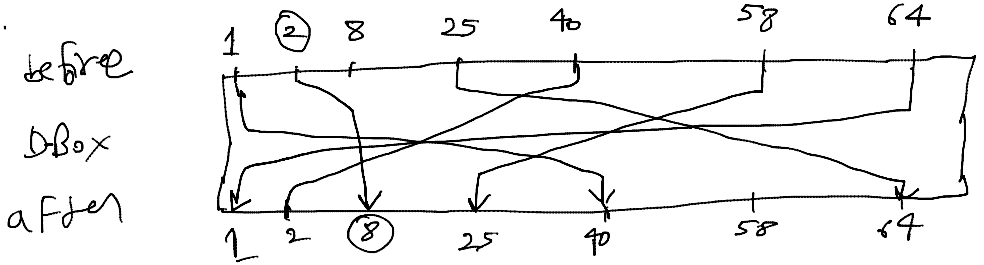
structure of DES:



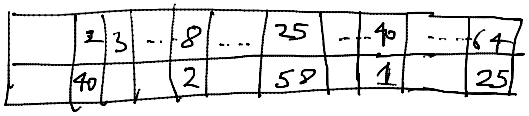


① Initial Permutation:

Initial & final Permutation are <u>Straight permutation</u> Box used to apply substitution operation on plaintext/Intermediatetext. [D-Box] (Straight)



D^{-1} Box (output)


3
3
8
25
40
64
40
2
59
1
25