$2^6 \bmod 6 = 1$

$3^6 \bmod 6 = 1$

$4^6 \bmod 6 = 1$

$5^6 \bmod 6 = 1$

A's Key : $X_A = 3$

$Y_A = 5^3 \bmod 7 = 6$

B's Key : $X_B = 4$

$Y_B = 5^4 \bmod 7 = 2$

secrete key (A) $= Y_B^{X_A} \bmod 7 = 2^3 \bmod 7 = 1$

secrete key (B) $= Y_A^{X_B} \bmod 7 = 6^4 \bmod 7 = 1$

Symmetric Algo

Encry

Decry $\rightarrow$ K $\downarrow$ K^{-1}] Hill

Asymmetric Algo

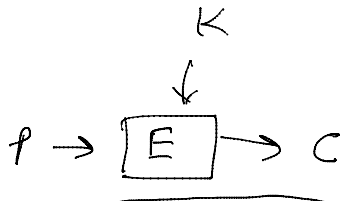
Encry — Pubic key of Receiver

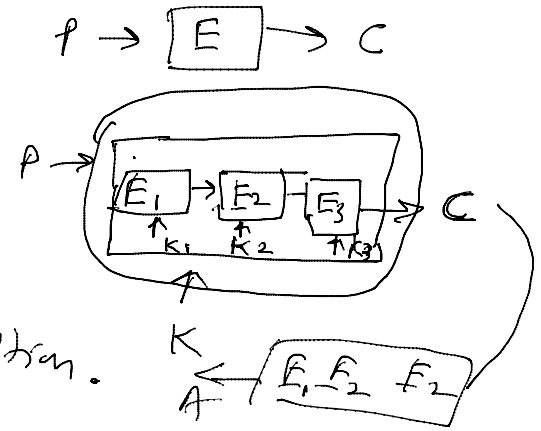
Decry — Private key of Receiver

Modern cryptography Algorithm (DES, AES, IDEA)

?

Feistel structure :



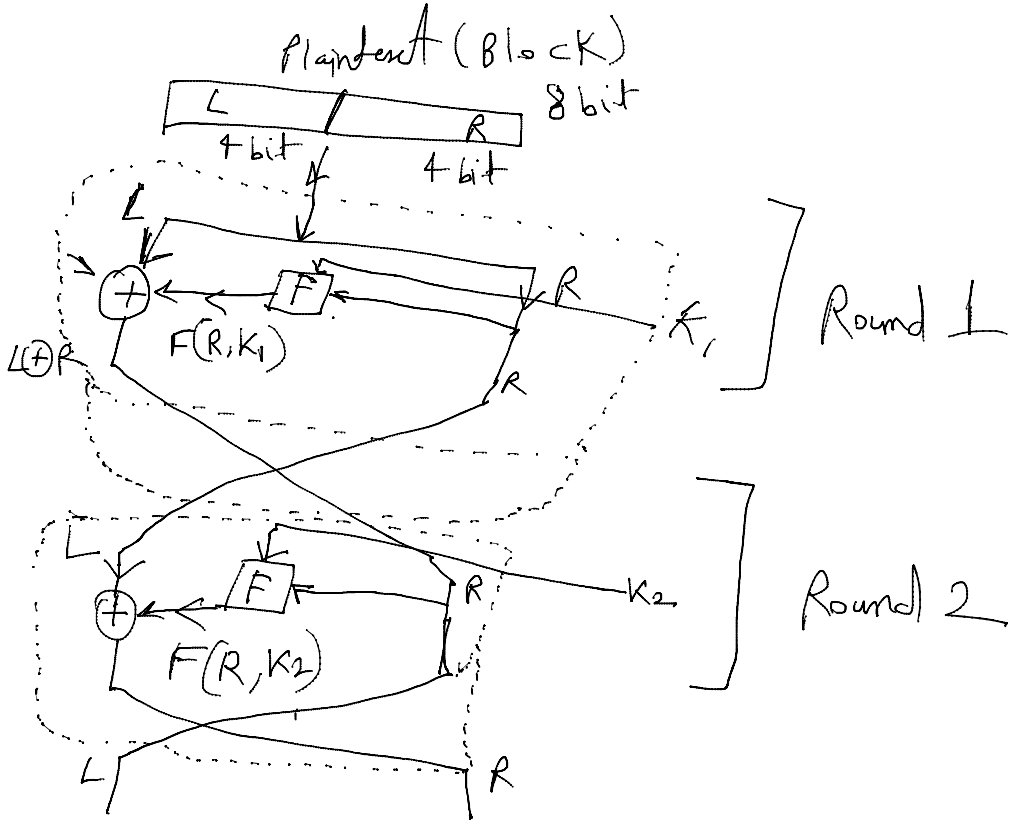


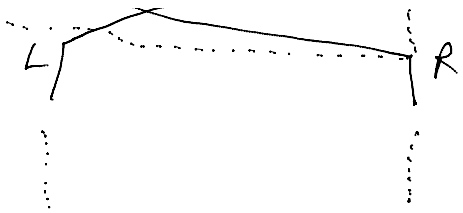
It is a design model from where many different block cipher are derived.

It uses same algorithm in both Encryption & decryption.

It uses multiple Round of processing of plaintext.

Each Round consist of a substition step followed by permutation step.





K = { K_1, K_2, K_3, K_4, K_5 ..... }

No. of sub Key = No. of Round

DES → 128 ← 128

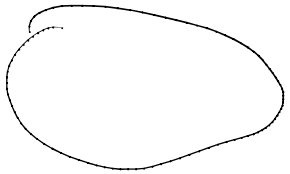
→ 64

→ 256

ASCII 7 bit

2^7 = 128

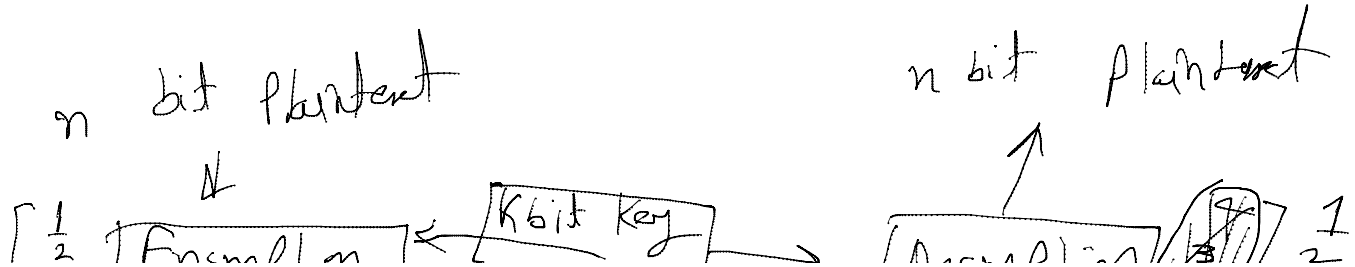
Modern symmetric key cryptography (cipher)

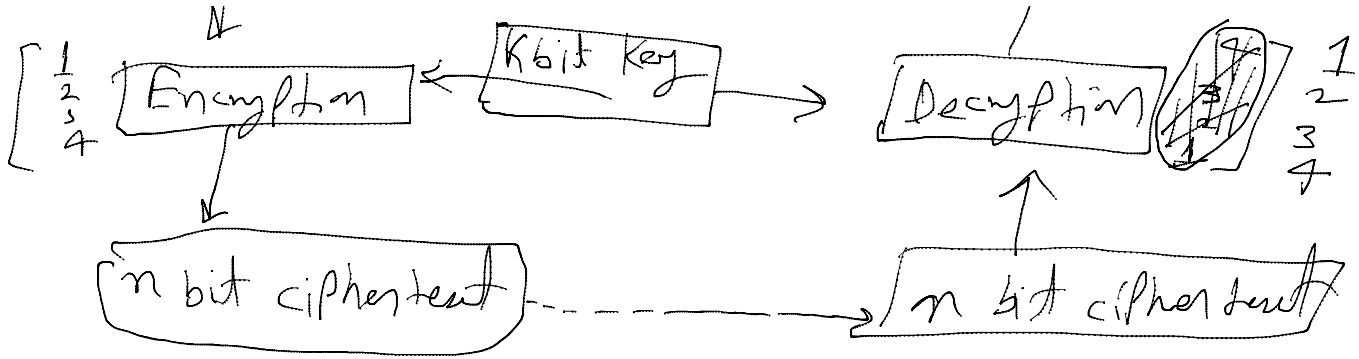


character oriented cipher: only for text based data

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

$64 = 800 \bmod 64 = 32$

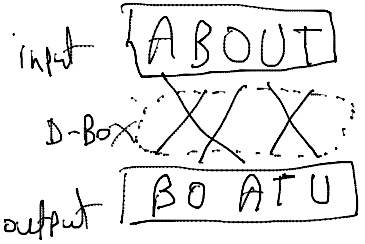
② Padding bits in last block =

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

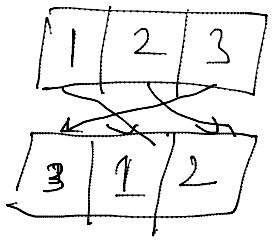
D-Box are three types:

(1) straight D-Box.

1	2	3

input size = 3

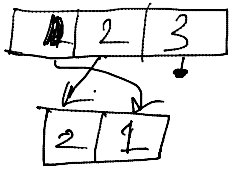
(a) straight D-Box :



input size = 3

output size = 3

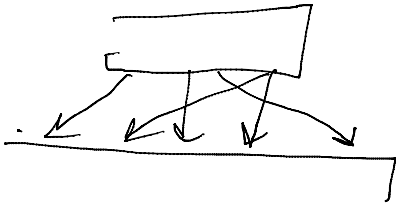
(b) Compression D-box :



Input size = 3

output size = 2

(c)



Expansion D-Box : 1 | 2 | 3 input = 3

1 | 3 | 2 | 3 | 2 output = 5