Key Generation → here 16 key is generated

4.2.3.1 Double DES :-

Since DES attack was vulnerable to brute force attack, variations of DES called multiple DES were introduced.

- use 2 DES keys (56+56) = 112 bit key

→ Double encryption occurs as follows

$P \rightarrow E(K_1, P)$

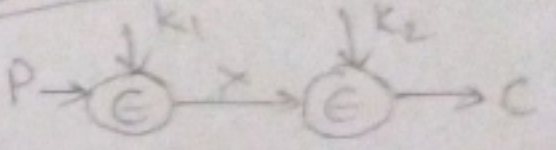
↓

$E(K_2, E(K_1, P)) = \text{Cipher}$

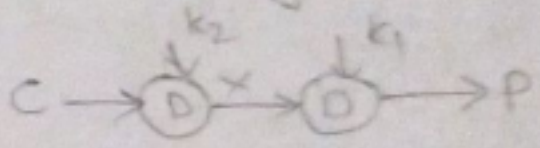
→ For Decryption

1st Decryption using key K_2 which produces single encrypted cipher text

- This 64 bit middle text is then decrypted using the key K_1 to get the plain text.

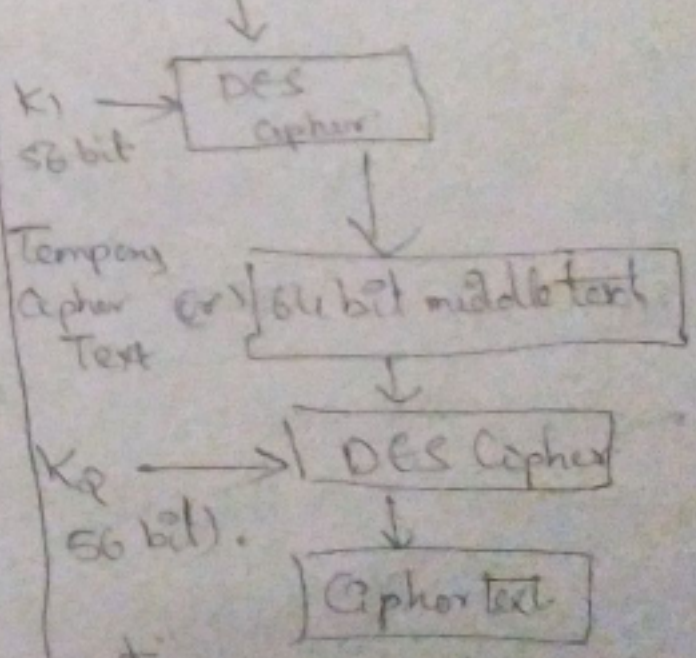


Encryption

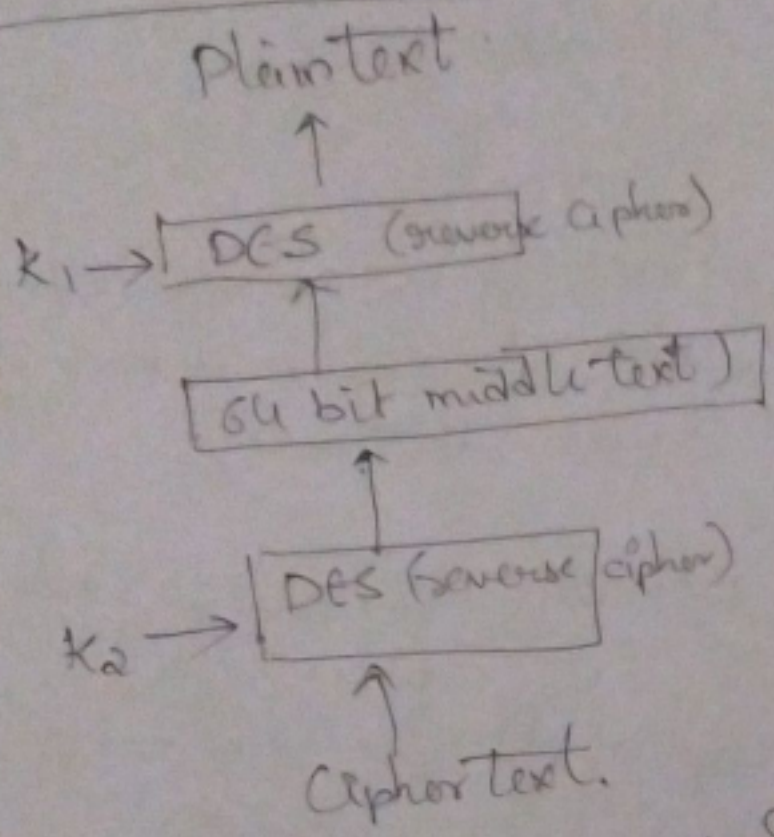


Decryption.

Data Encryption



Double DES Decryption:-



The decryption, key are applid in reverse order

$$\text{Plain} = D(K_1, D(K_2, C))$$

↓ First this will happen

Drawback of Double DES

Meet in the middle attack.

This attack involves encryption from one end & decryption in another end then "making the results in the middle and ~~reverse~~ hence the name

MIM attack

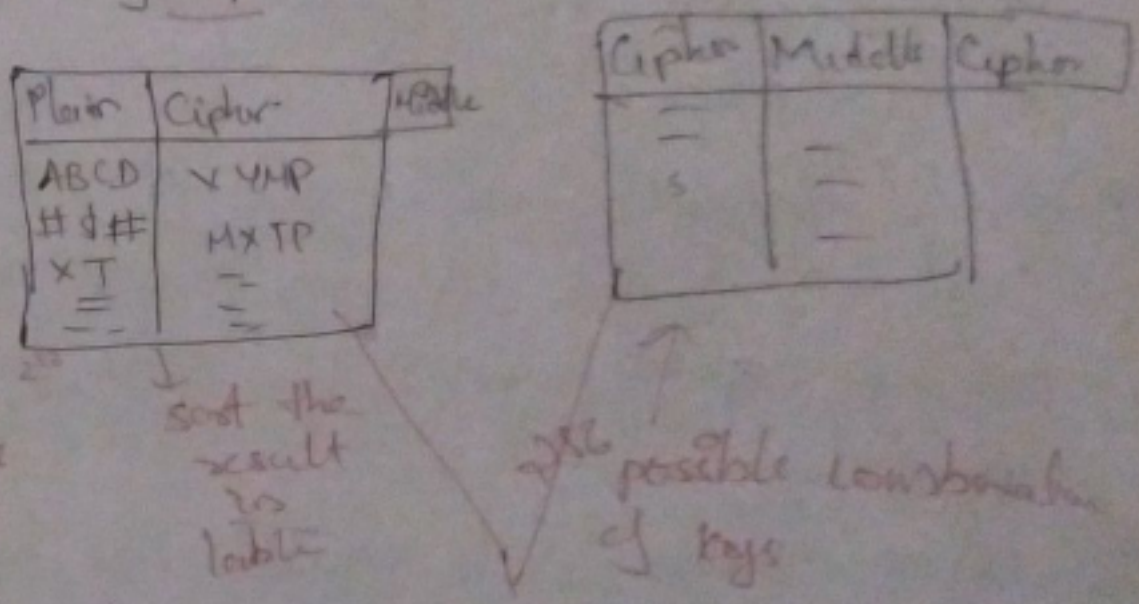
Some pairs

plain text known & Cipher text known

↓ ↓

Encrypt pairs for all 2^{56} possible values of K_1

decrypt pairs of all 2^{56} possible value of K_2



→ (K_1, K_2)

→ (K_1, K_2)

We will compair these values with values of the 1st table computed earlier.

$$\text{Decrypt}(K_2, C) = \text{Encrypt}(K_1, P)$$

$\therefore (K_1, K_2)$ is the key pair used.

This attacks requires some pairs of plaintext / ciphertext pairs.

Let us assume plaintext = P ; Ciphertext = C.

This attack proceeds as follows:

(i) Encrypt (P) for all 2^{56} possible value of K_1 & store the results in a table & sort it.

(ii) Now, decrypt (C) using all 2^{56} possible values of K_2 - As each result is produce, check against the table for a match.

(iii) When there is a match, we have located a possibly correct pair of keys.

Note, Now more than 1 pair keys may result in a match, but these no. of pairs will be small, we should try each possible pair of keys.

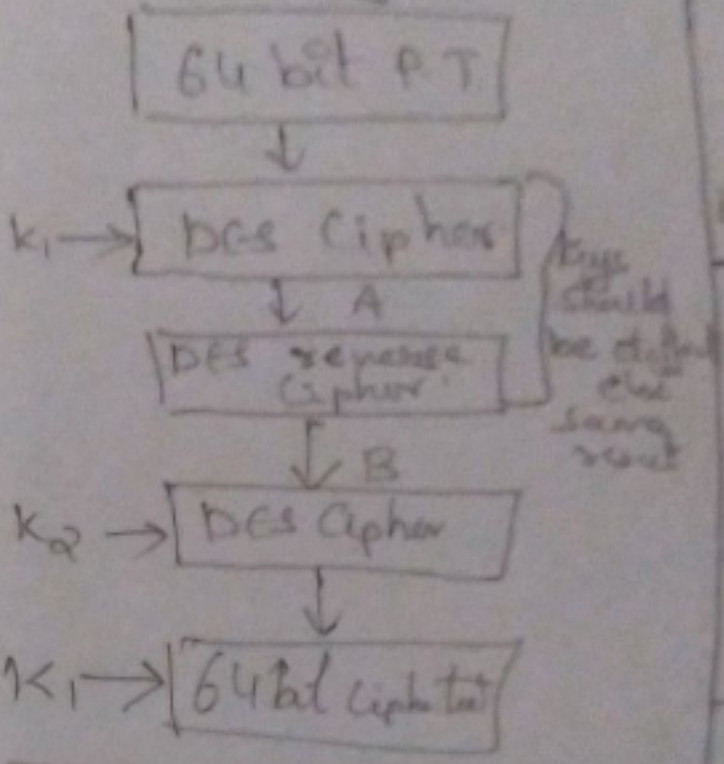
- So, it takes twice as long to break double DES using brute force attack

Because, DES has 2^{56} bit security, Double DES has $2 \times 2^{56} = 2^{57}$ key security

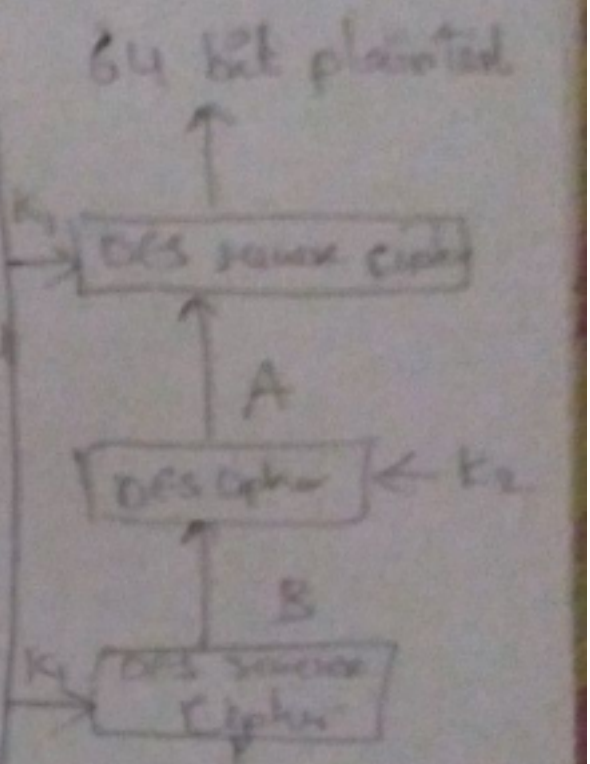
TRIPLE DES : 3DES

2 or 3 keys are used

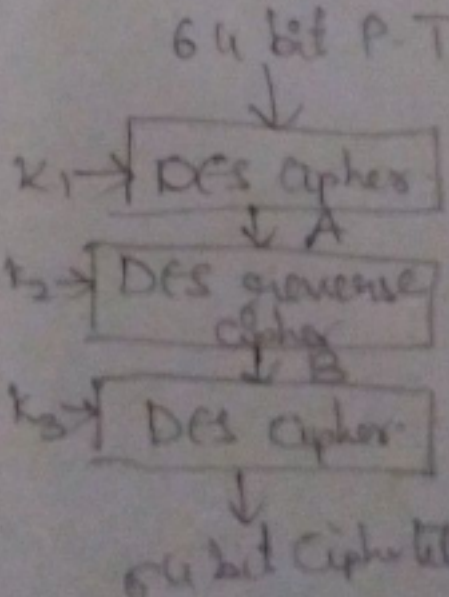
- Much stronger than 2DES.



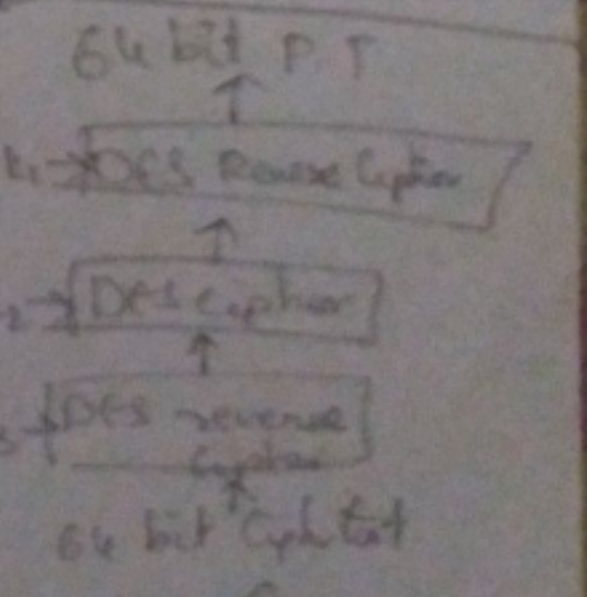
Encryption using 2 keys



Decryption using 2 keys



Encryption by 3 keys



Decryption using 3 keys.