Decryption
Reverse process.

DES Analysis:-
properties
(i) Avalanche effect
(ii) Completeness effect

Avalanche effect

It means a small change in plain Text (or key) should create a significant change in cipher text.

Same key { plain Text 1 → Cipher Text 1 ; plain Text 2 → cipher Text 2] differ only by one bit around 29 bits are different

eg

plain Text 1 = 0000000000
Cipher Text 1 = 4789FD476E

Key = 2223451298

plain Text 2 = 0000000001
Cipher Text 2 = 0A4ED5C15A

Although the 2 plaintext blocks differ only in the right most bit, ~~the cipher text~~ there is a significant change in ciphertext blocks.

DES has been proved to be strong with regards to this property

completeness effect

It means that each bit of cipher text needs to depend on many bit on plain Text.

The confusion and Diffusion produced by P-Boxes and S-boxes in DES show a very strong completeness effect

Multiple DES

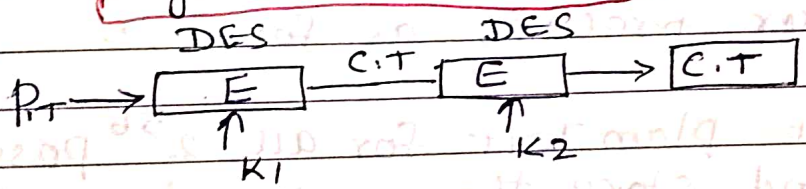
1. Double DES (2 DES) — Triple DES with 2 keys
2. Triple DES (3 DES) — " " " 3 "

Sine DES attack was vulnerable to brute force attack, variations of DES called Multiple DES were introduced.

1. Double DES (2 DES)

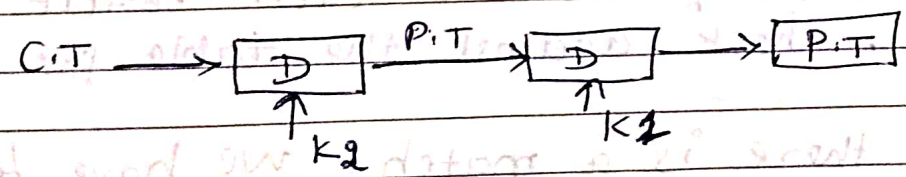
The simplest form of multiple encryption has 2 encryption stages and 2 keys.

Key = 56 x 2 = 112 bits.



$$C = E(K_2, E(K_1, P))$$

Decryption



$$P = D(K_1, D(K_2, C))$$

→ Double DES uses 2 keys k_1 and k_2
→ It performs DES on the original plain text using k_1 to get the encrypted text
→ It again performs DES on the encrypted text, but this time with other key k_2.
→ The original plain text encrypted twice with 2 different keys.

Draw back of ~~Dobad~~ Double DES.

Meet-in-the-middle attack. (MIM attack)

This attack involves encryption from one end and decryption from the other end and then "matching the results in the middle" and hence the name.

This attack requires knowing some plain text cipher text pairs.

let us assume plain text = P
cipher text = C.

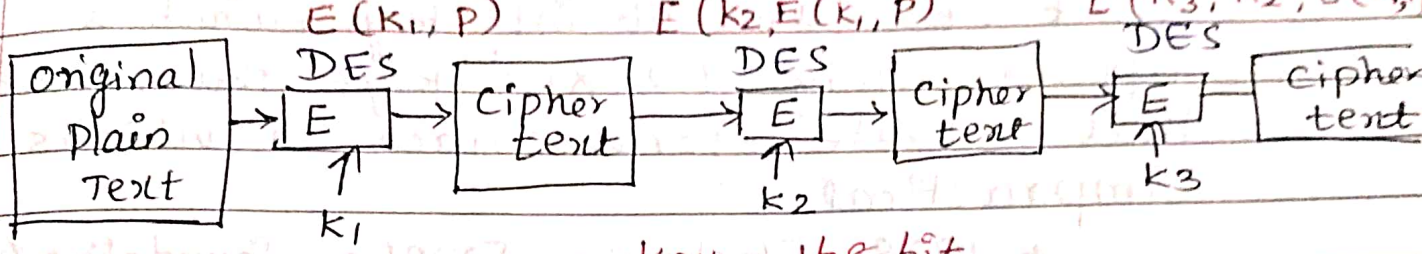
The attacker proceeds as follows :-

(i) encrypt plain text for all 2^{56} possible values of K_1 and store the results in a table and sort it.
(ii) Now decrypt cipher text using all 2^{56} possible value of k_2. As each result is produced, check against the table for a match.
iii) When there is a match, we have located a possibly correct pair of keys.

Triple DES with 3 keys.

→ The plain text is first encrypted with a key K_1, then encrypted with a second key K_2, and finally a third key, K_3.

→ Where K_1, K_2, K_3 are all different from each other.



Key = 168 bit.

Triple DES with Two keys

1. Encrypt the plain text with K_1 $E(K_1, P)$
2. Decrypt the output of step 1 with K_2. $D(K_2, E(K_1, P))$
3. Finally encrypt the output of step 2 again with K_1.

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, C)))$$