Multiple encryption with DES

- DES is vulnerablee to brute force attack.
- Alternative idea
  encrypt multiple times with diffrent Keys

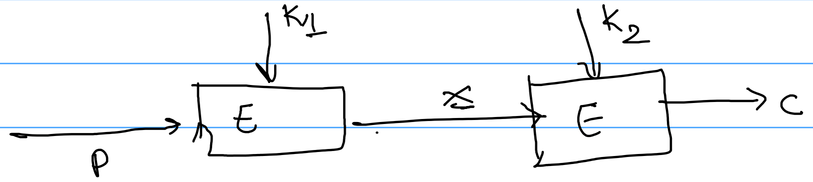
Options

(I) - Double DES : not much better than Single DES

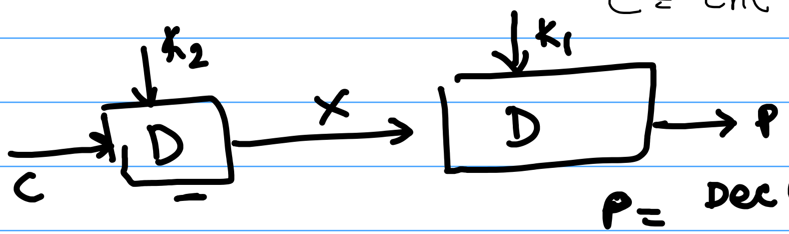
(II) - Triple DES (3 DES with 2 Keys) .

(III) - Triple DES with 3 Keys

2DES



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



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

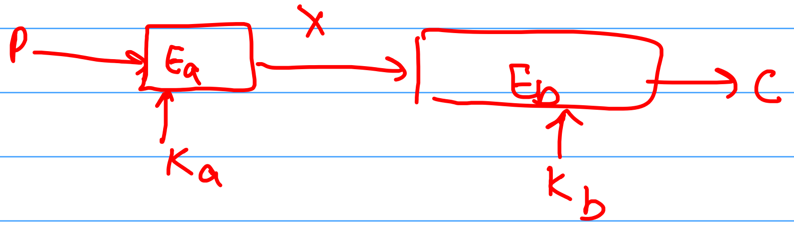
2X56 bit Keys meaning 112 - bit Key length.

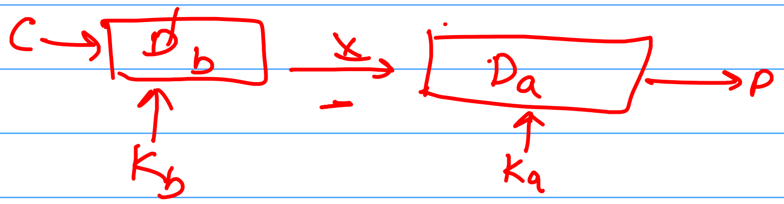
Meet in the Middle attack

↳ applies for any block encryption cipher

↳ Known-plaintext attack
(P.T, C.T)

- MITM attack, it is possible to break cipher which have two or more secret keys for multiple encryption using the same algo.





$$C = En_b(K_b, En_a(K_a, P))$$

$$P = De_a(K_a, D_b(K_b, C))$$

2^{56}

$$D_b(K_b, C) = \underline{E_a(K_a, P)}$$

1. Create a table with all possible value for one side of the equ^n.

↓

possible ciphertext of the plaintext P.

No. of rows in the table = no. of possible secret key.

2. Calculate values of $D_b(K_b, C)$ for the second side of the equ^n

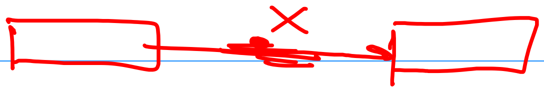
- If there is a match of intermediate CT, it is highly possible that the key used to encrypt the PT and key used to decrypt the CT are two encryption key used for blockcipher crytoanalysis (key)

- MITM → passive attack

  ↓ can not alter the message or send their own.

- not possible for average hacker and is more likely to be used by organizations that can accomdate the storage required to carry it out.

the



Meet in the Middle vs man in the middle

attacker is in the middle of two communicating users.

↓ Cryptoanalysis passive attack

↳ active attack

↳ capable of intercepting, relying and possibly altering messages.