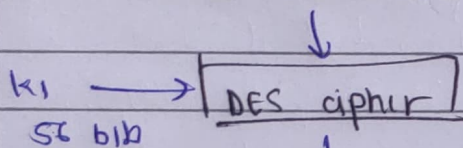


5) Double DES for Brute force & Meet in the Middle① Brute force  $\Rightarrow$  uses DES twice

$$\text{Key} = 2 \times (56 + 56) = 112 \text{ bit key}$$

$$\text{Security} = 2 \times 2^{56} = \boxed{2^{57}} \text{ combination of key's to be security } (2^{56} < 10^{17})$$

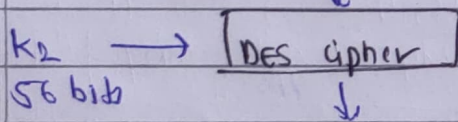
64 bit Plaintext



$$P \rightarrow E(K_1, P)$$

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

(64 bit middle text) temporary ciphertext



ciphertext

② Meet in the middle - This attack involves encryption from 1 end & decryption from other end and then

"matching the results in middle" & hence the name.

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

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

(i) encrypt "P" for all  $2^{56}$  possible values of  $K_1$  & store result in table & sort it

(ii) Now decrypt "C" using all  $2^{56}$  possible values of  $K_2$ . As a ~~result~~ decryption, check against table for match.

(iii) When there is match we pair the key, & try for all possible pair of keys.

\*

Triple DES - No more men in middle attack

→ Another

$$\text{Security} = (56 + 56 + 56) = 168 = \text{Key}$$

$$2^{56} \times 2 \times 2 = [2^{58} \text{ security}]$$

Key ↑ & Security ↑

DES cipher

DES cipher

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