Double DES

$$C = E(K_2, E(K1, P))$$

$$P = D(K1, D(K2, C))$$

Key length = 56 × 2
= 112 bits

⇒ Suppose

$$E(K2, E(K1, P)) = E(K3, P)$$

Meet in the Middle Attack

$$X = E(K1, P) = D(K2, C)$$

Given Known pair (P, C)

① Encrypt P for all values of K1 i.e 2^{56}
Put in table and sort by X

② Decrypt C for all values of K2 i.e 2^{56}
check result against table for Match.

③ if match occurs, test two keys against new plain-cipher text pair.
if produce correct cipher accept as correct keys.

⇒ The plaintext require 2^{56} effort

Same as DES 2^{55}

Multiple Encryption

$$C = E(K1, D(K2, E(K1, P)))$$

$$P = D(K1, E(K2, D(K1, C)))$$

Known PlainText Attack

(1) obtain n (P, C) pairs and sort by P.

(2) Pick any value for 'a' & produce P_i

2^{56} keys $K1 = i$

$P_i = D(i, a)$ (Table 1 match)

$B = D(i, C)$ (Table 2 key1, B)

(3) calculate K2

Pick any value of 'a'

$B_j = D(j, a)$

$K2 = j = 2^{56}$ keys

if match i and j are keys

(4) Test keys (i, j) on other plain-cipher

if no pair find then select new value of 'a' & Repeat Algo