MULTIPLE DES:
2DES
3DES

2DES

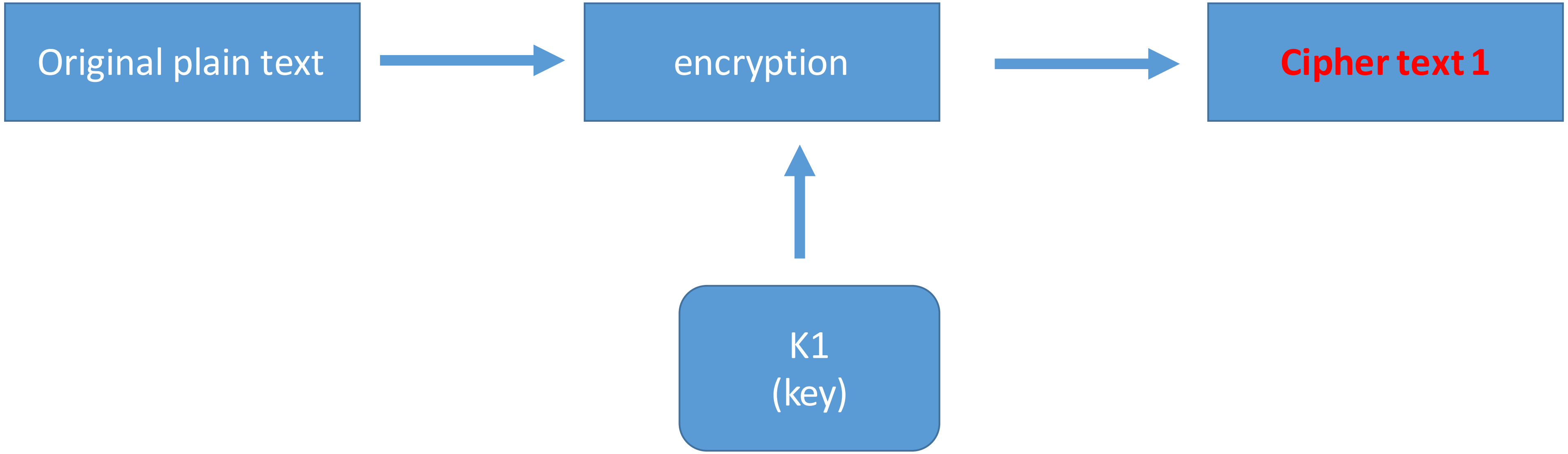
In this approach, we use two instances of DES ciphers for encryption and two instances of reverse ciphers for decryption.

Each instances use a different key.
The size of the key is doubled.
There are issues of reduction to a single stage.
However, double DES is vulnerable to meet in the middle attack
Given a plaintext P and two encryption keys K1 and K2, a cipher text can be generated as,

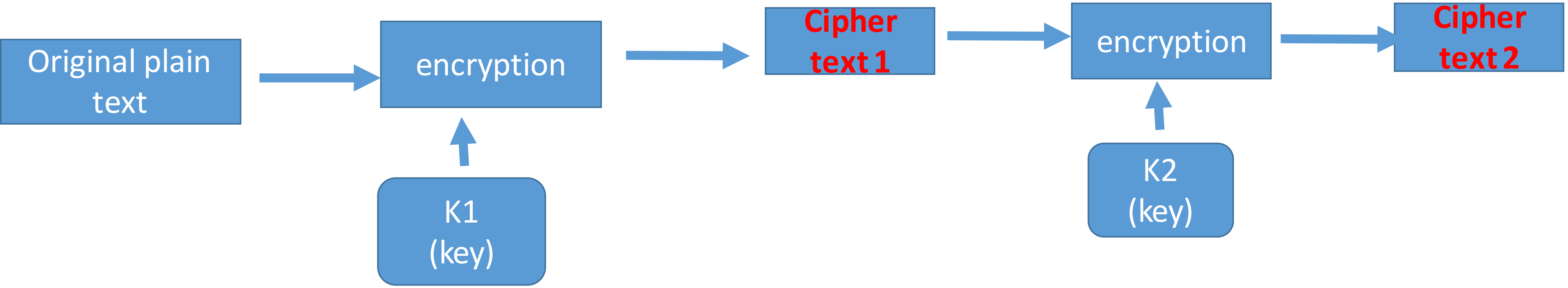
C=E(K2,E(K1,P))
Decryption requires that the keys be applied in reverse order,

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

2DES (ENCRYPTION PROCESS)



Double DES is represented as :
C1=E(K1,P)



Double DES is represented as :

C1=E(K1,P)

C2=E(K2,C1)

There for: C2=E(K2,E(K1,P))

Where:

K1= KEY1

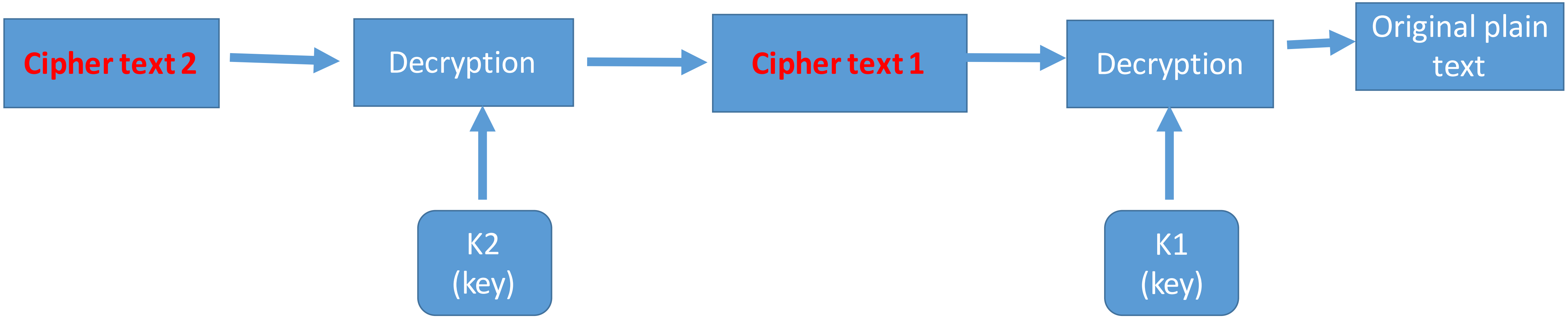
K2=KEY2

C1=FIRST CIPHER TEXT

C2=FINAL CIPHER TEXT

E=ENCRYPTION PROCESS

2DES (Decryption process)



Double DES decryption process is represented as :

C1=D(K2,C2)

P=D(K1,C1)

There for:

P=D(K1,D(K2,C2))

Where:

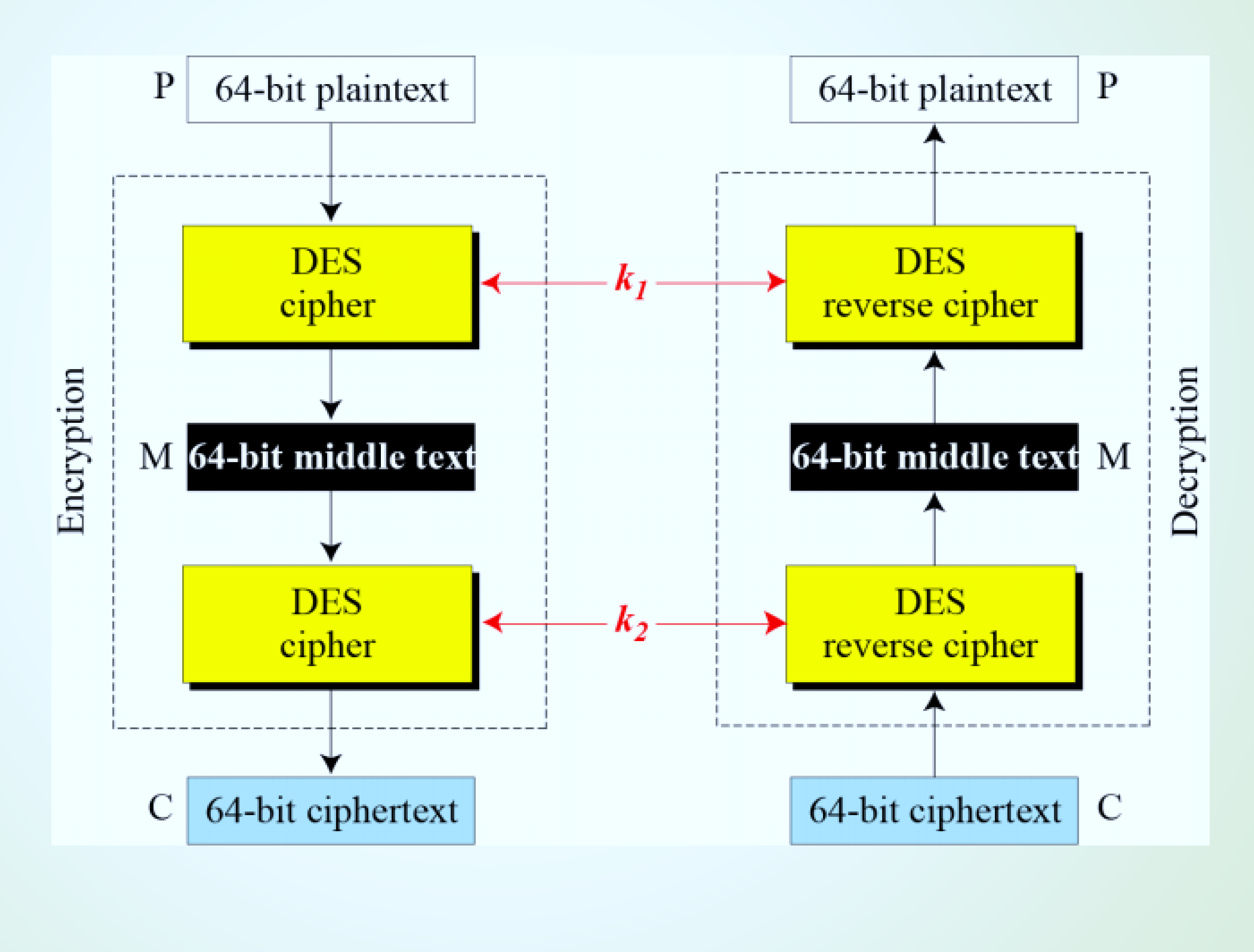
K1= KEY1

K2=KEY2

C1=FIRST CIPHER TEXT

C2=FINAL CIPHER TEXT

D=DECRYPTION PROCESS


P
64-bit plaintext
64-bit plaintext
P
Encryption
DES
cipher
k_1
DES
reverse cipher
Decryption
M
64-bit middle text
64-bit middle text
M
DES
cipher
k_2
DES
reverse cipher
C
64-bit ciphertext
64-bit ciphertext
C

The middle text, the text created by the first encryption or the first decryption, M, should be same

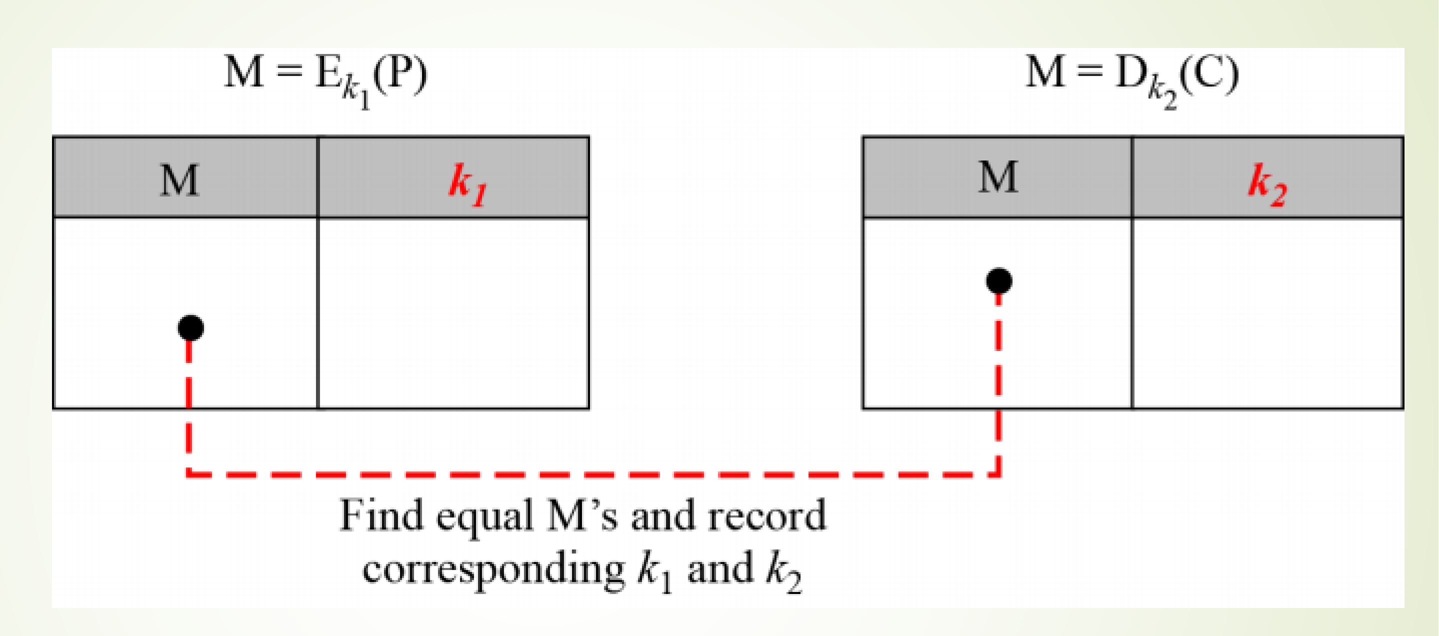
M=EK1(P) and M=DK2(C)
Encrypt P using all possible values of K1 and records all values obtained for M.

Decrypt C using all possible values of K2 and records all values obtained for M.

Create two tables sorted by M values.

Now compares the values for M until we finds those pairs of K1 & K2 for which the value of M is same in both tables

NOTE:
Double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.



Note:

Instead of using 2112 key search tests, we have to use 256 key search tests two times.

Moving from a Single DES to Double DES, we have to increase the strength from 2^56 to 2^57