Double DES & Triple DES

Prepared by : Sharma Hemant

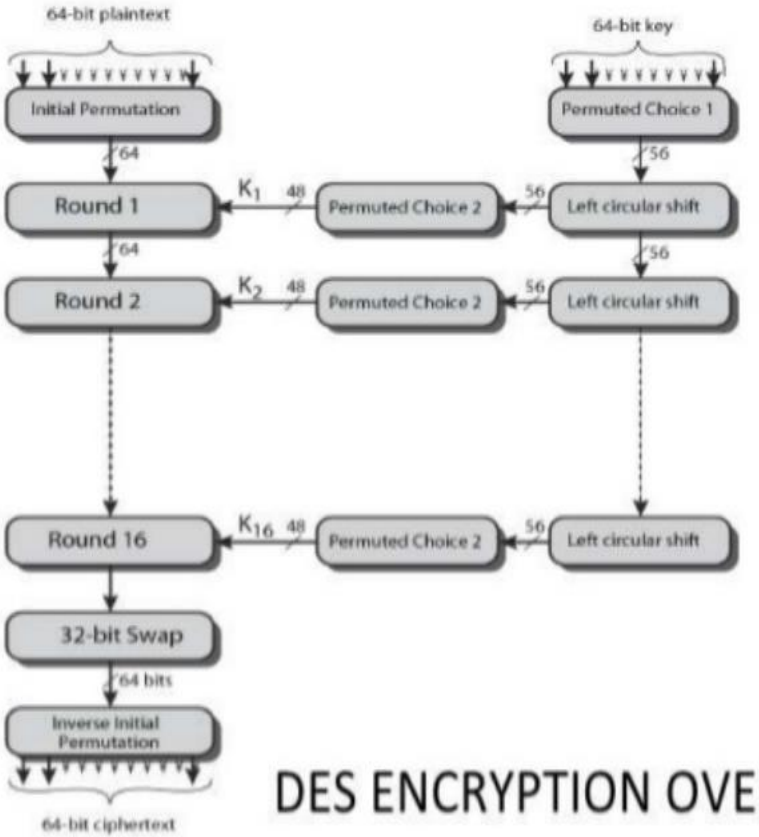
hemantbeast@gmail.com

Contents

- DES Overview
- Double DES
- Triple DES with 2-key encryption
- Triple DES with 3-key encryption

Clip slide

DES Overview



DES Overview

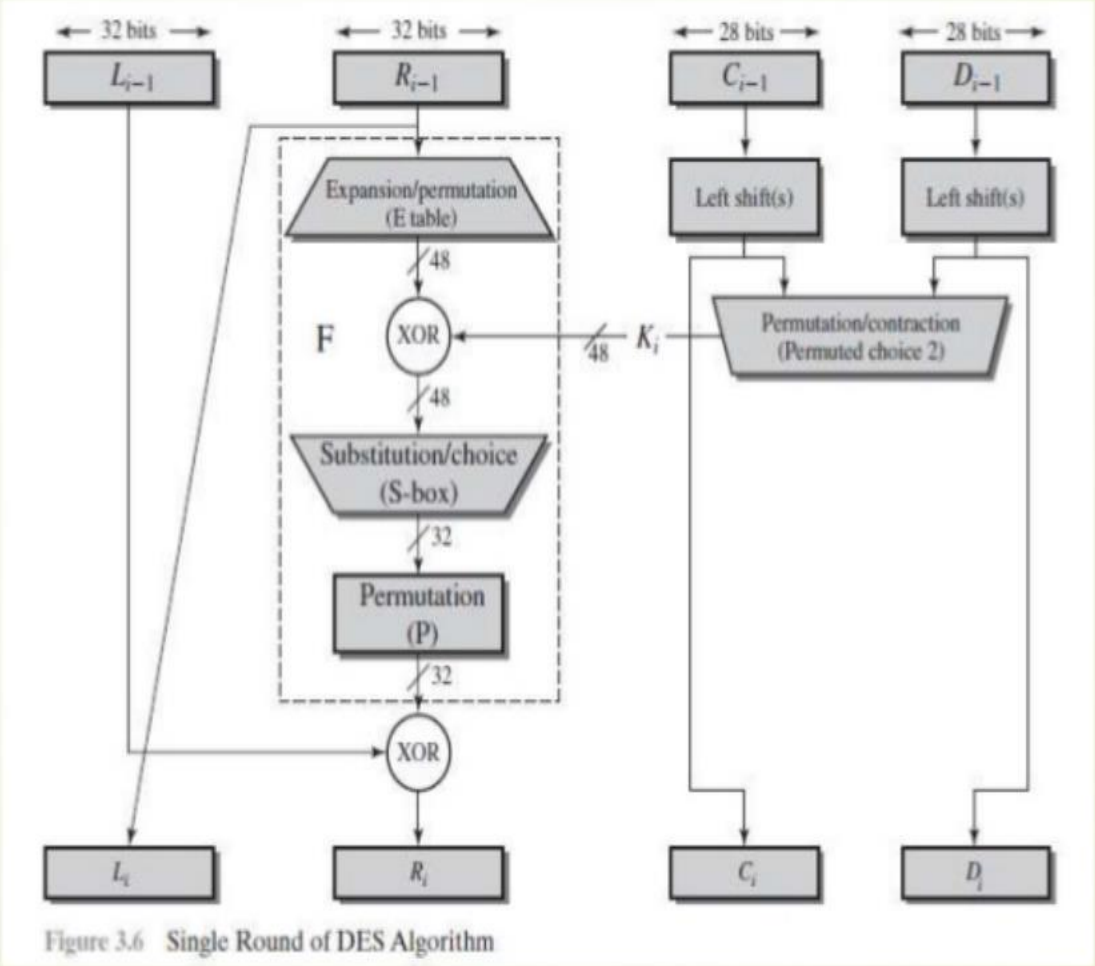


Figure 3.6 Single Round of DES Algorithm

Double DES

- 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 single stage.
- However, double DES is vulnerable to meet-in-the-middle attack.

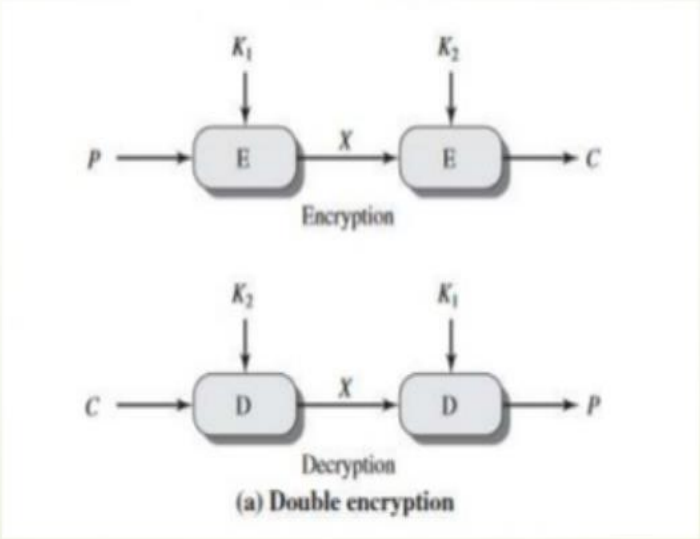
Double DES

- Given a plaintext P and two encryption keys K_1 and K_2, a cipher text can be generated as,

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

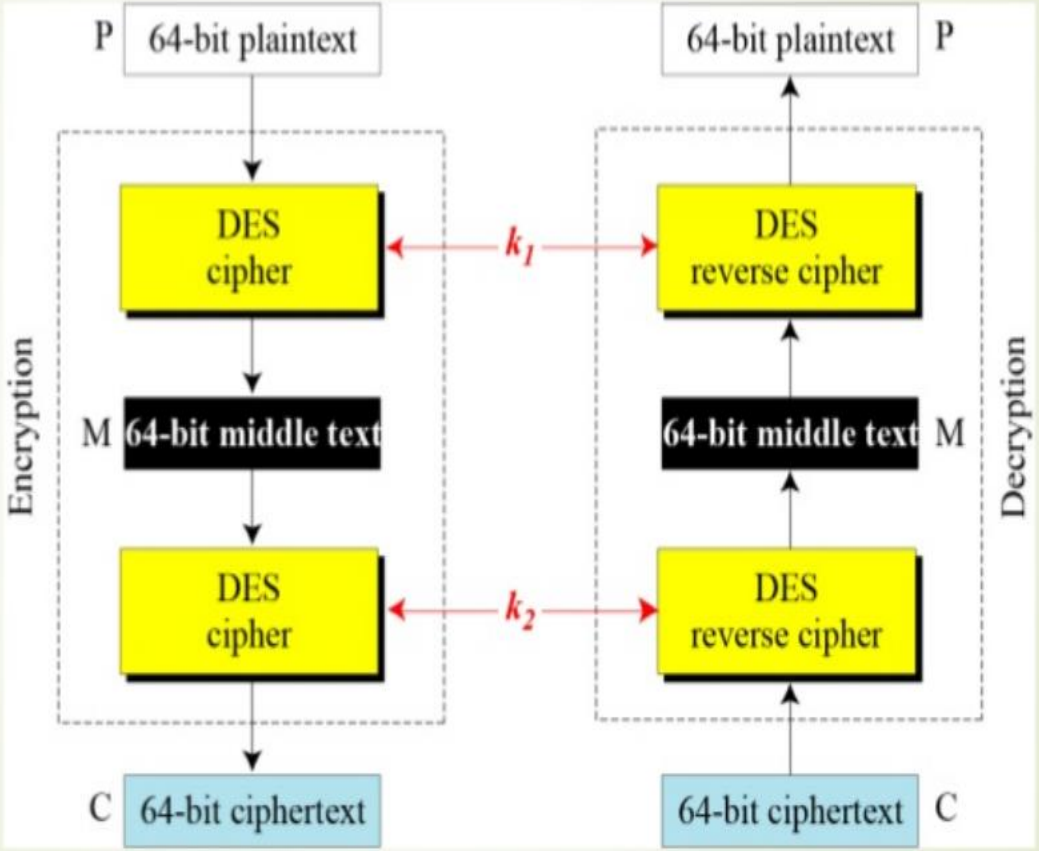
- Decryption requires that the keys be applied in reverse order,

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



(a) Double encryption

Meet-in-the-middle attack



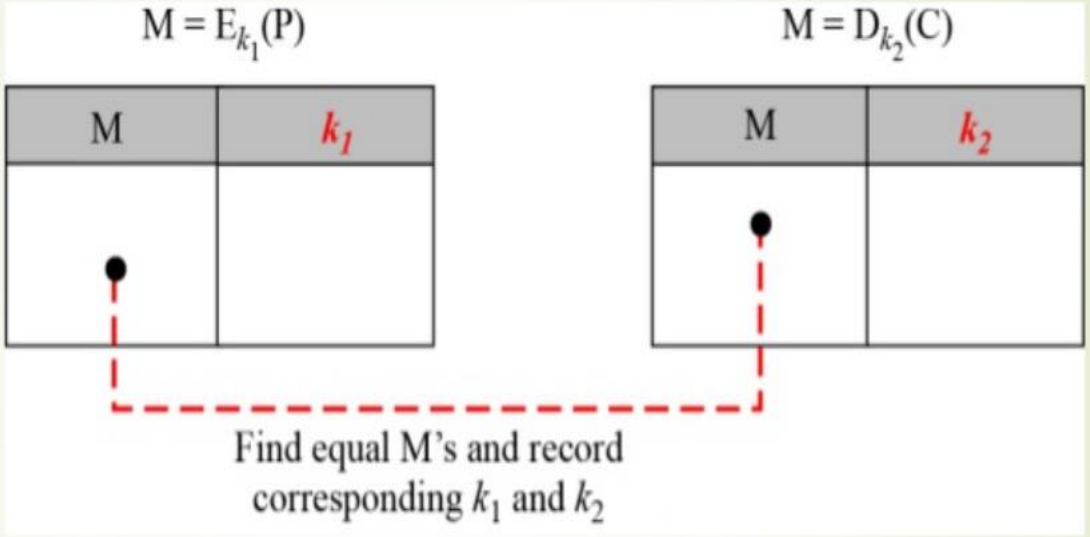
Meet-in-the-middle attack

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

$$M = E_{K1}(P) \qquad M = D_{K2}(C)$$

- Encrypt P using all possible values of K_1 and records all values obtained for M.
- Decrypt C using all possible values of K_2 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 K_1 & K_2 for which the value of M is same in both tables.

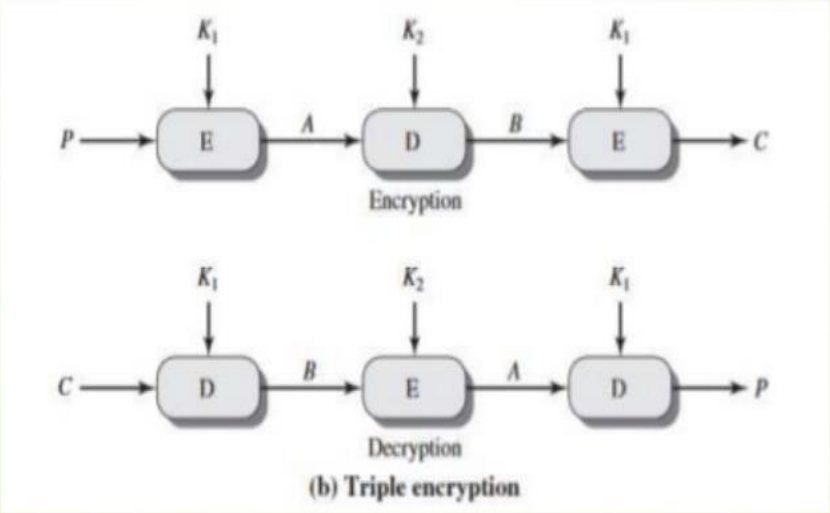
Meet-in-the-middle attack



- Instead of using 2^{112} key search tests, we have to use 2^{56} key search tests two times.
- Moving from a Single DES to Double DES, we have to increased the strength from 2^{56} to 2^{57}.

Triple DES with 2-key

- Use three stages of DES for encryption and decryption.
- The 1st, 3rd stage use K_1 key and 2nd stage use K_2 key.
- To make triple DES compatible with single DES, the middle stage uses decryption in the encryption side and encryption in the decryption side.
- It's much stronger than double DES.



(b) Triple encryption

Triple DES with 2-key

- The function follows an encrypt-decrypt-encrypt (EDE) sequence.

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

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

- By the use of triple DES with 2-key encryption, it raises the cost of meet-in-the-middle attack to 2^{112}.
- It has the drawback of requiring a key length of $56 \times 3 = 168$bits which may be somewhat unwieldy.

Triple DES with 3-key

- Although the attacks just described appear impractical, anyone using two-key 3DES may feel some concern.
- Thus, many researches now feel that 3-key 3DES is the preferred alternative.
- Use three stages of DES for encryption and decryption with three different keys.
- 3-key 3DES has an effective key length of 168 bits and is defined as,

$$C = E(K_3, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_3, C)))$$

Triple DES with 3-key