1. Triple Data Encryption Standard (3-DES)

Triple DES was introduced to improve on the security of DES. This encryption technique uses three stages of DES for encryption & decryption on same plaintext.

There are mainly 2 versions of Triple DES known as 3-key Triple (3TDES) and 2-key Triple DES (2DES)

- **Triple DES with two keys** –

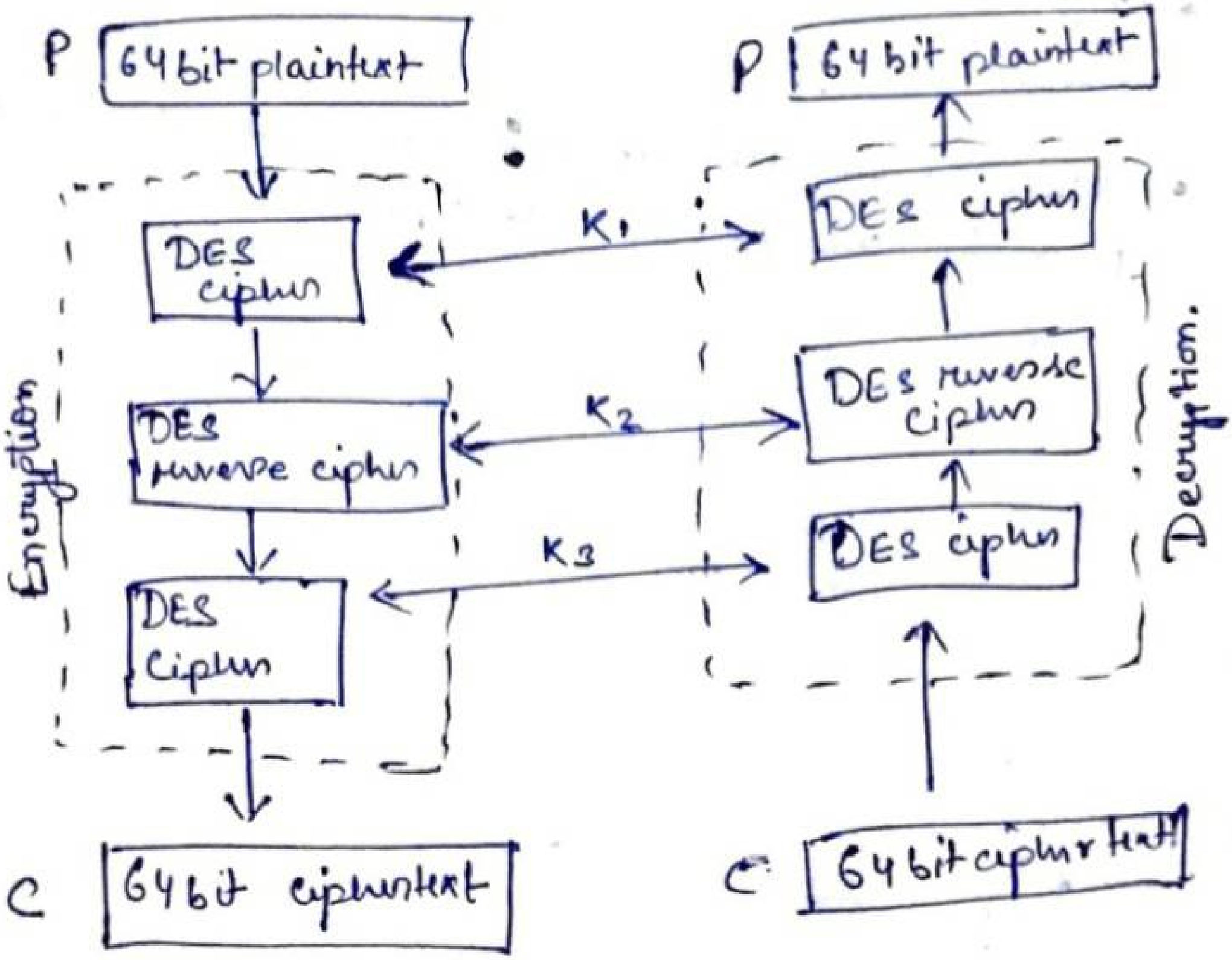
There are only two keys; K_1 & K_2. The first and the third stage use K_1, second stage uses K_2. In other words, users encrypt plaintext blocks with key K_1, then decrypt with key K_2 & finally encrypt with K_1, again.

- **Triple DES with three keys** :-

In this version there are three different keys, K_1, K_2 & K_3. Due to the design of 3-DES as an encrypt – decrypt – encrypt process, it is possible to use 3TDES implementation for single DES by setting K_1, K_2, & K_3 to be the same value.
This provide backward compatibility.

The encryption - decryption process is as follows

1) Encrypt the plaintext blocks using single DES's with key K_1.
2) Now decrypt the output of step 1 using DES with key K_2.
3) Finally, encrypt the output of step 2 using single DES with key K3.
4) The output of step 3 is the ciphertext
5) Decryption of ciphertext is a reverse process. Use first decrypt using K_3, then encrypt with K_2 & finally decrypt with K_1.



1. 3-DES :

3DES officially known as Triple Data Encryption Algorithm (TDEA) it is most commonly referred to as 3DES. This is because 3DES algorithm uses data encryption standard (DES) cipher three times to encrypt its data.

DES is a symmetric key algorithm based on Feistel Network. As a symmetric key cipher, it uses the same key for both encryption & decryption process. The Feistel Network makes both of these process almost exactly the same, which results in an algorithm that is more efficient to implement.

It has 64 bit, block & key size. but in practice the key only grants 56 bits of security. 3DES was developed as a more secure alternative because of DES's small key length. In 3DES, DES algorithm is used three times with three keys, It is considered secure only if three separate keys are used

- key one is used to encrypt plain text
- key two is used to decrypt the text that had been encrypted by key one
- key three is used to encrypt the text that was decrypted by key two.

There are 3 different keying options / configurations

(1) Using three different keys / is most secure
(2) Using first & third key same but is less secure
(3) Using three identical keys, would come as normal DES.

* Process :

Encryption :

1. Plain text enters / encrypted using key L. as follows.
   - key schedule - 16 subkeys are derived from key one.
   - Initial Permutation
   - Block is split into right & left halves.
     → The right half is sent through f function
     ⇒ Expansion permutation
     ⇒ XOR the subkey for the round
     ⇒ Substitution
     ⇒ Permutation
     → The left side is sent to f function
     - Take XOR of both
     Make ~~left~~ old ~~R~~ right side new left side / result
     new right side.

Repeat for 15 more rounds.

. Combine left & right side of block together.
. Final Permutation.

2. Take the output & send it through decryption process with key two.

- key schedule - 16 subkeys are derived from key two.
- Initial Permutation
- Block is split into right & left halves
  - => Expansion Permutation
  - => XOR with the subkey for round 16.
  - => Substitution
  - => Permutation.
- XOR with result of f function of left side.
- Make old right side new left side & result above as new right side

Repeat bit for more 15 times

- Combine left & right block together
- Final Permutation.

3. We run encryption process with key three again same as in part 1.

The final result is 3DES ciphertext.

* Real World Example :

Some real world example includes implementation in

- Microsoft Office
- Firefox
- EMV payment systems

* Advantages:

- It is a counter to meet in the middle attack. with three different keys.
- It increases cost of known plaintext attack 2^{112}. which is beyond practical now.
- In 3DES, cost of differential cryptanalysis suffer an exponential growth., compared to single DES.

* Disadvantages:

- keying options 2 & 3 are are more vulnerable to both known plaintext & chosen plaintext.
- If we used 3 different keys, it will increase the key length to $3 \times 56 = 168$ bits.

Indu Singh, AP, CSE, DTU