

ASSIGNMENT-03

* Triple DES

- It is an encryption algorithm based on the original Data Encryption Standard. It is a symmetric encryption algorithm that uses multiple rounds of DES to improve security.
- Known as triple DES because it uses the DES cipher which takes three times to encrypt its data.

→ Working of Triple DES

Encryption process of triple DES involves:

(i) key generation:

First step in which three keys that are unique, generated using a key derivation algorithm.

(ii) Initial permutation:

It involves the rearrangement of bits of plain text according to a predefined permutation table.

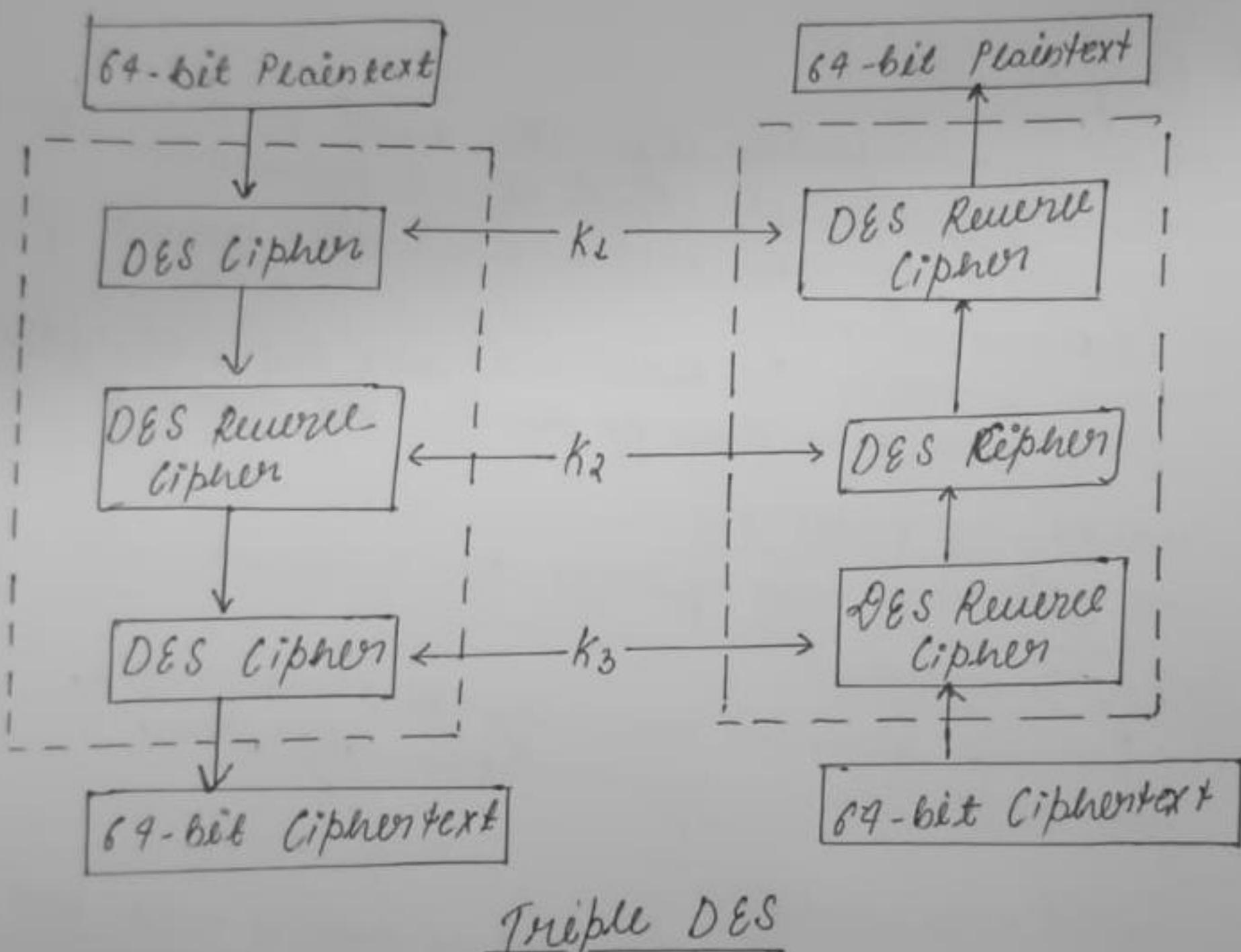
(iii) Three rounds of encryption:

It consists of multiple rounds typically 48 rounds in total. In this step, the plain text is processed three times and gets encrypted, each time we take use of a different key, to create three layers of encryption.

(iv) Final Permutation

It completes the Triple DES encryption process.

In this step, the resulting cipher text block undergoes a final permutation (FP) operation which is the inverse of initial permutation. It returns all the bits of the cipher text block to their original order.



* Advantages:

1. Provides three layered encryption technique which provides enhanced security features.
2. Offers backward compatibility with DES which means it can use legacy system that DES uses.
3. It supports variable key sizes, which led to enhanced security.

- * Block Cipher modes
- 1. Electronic Codebook (ECB): Each block of plaintext bits is encoded independently using the same key.
- 2. Cipher Block Chaining (CBC): The input to the encryption algorithm is XOR of the next block of plaintext and preceding block of cipher text.
- 3. Cipher Feedback (CFB): Input is processed 8 bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.
- 4. Output Feedback (OFB): Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.

Mode	Security	Error propagation	Repeated plaintext handling
ECB	weak (patterns leak)	Error stays in block only	Repeated blocks visible
CBC	stronger (chaining reduces repetition)	current + next block corrupted	Repetition hidden
CFB	strong, like stream cipher	Error affects bits of one block + some next bits	Repetition hidden
OFB	strong (like stream cipher)	Error affects only same bit position	Repetition hidden

- * Role of initialization vector (IV)
- CBC: IV ensures the first plaintext block doesn't encrypt to the same ciphertext for identical plaintexts. Must be unpredictable.
- CFB: IV seeds the feedback chain; must be unique.
- OFB: IV seeds keystream; if reused, keystream repeats \rightarrow catastrophic vulnerability.
- * When to prefer which mode:
- ECB \rightarrow Avoids unless encrypting a single block of random data (e.g. keys)
- CBC: But for large sequential files or databases
- OFB: Ideal for noisy environments (minimal error propagation).