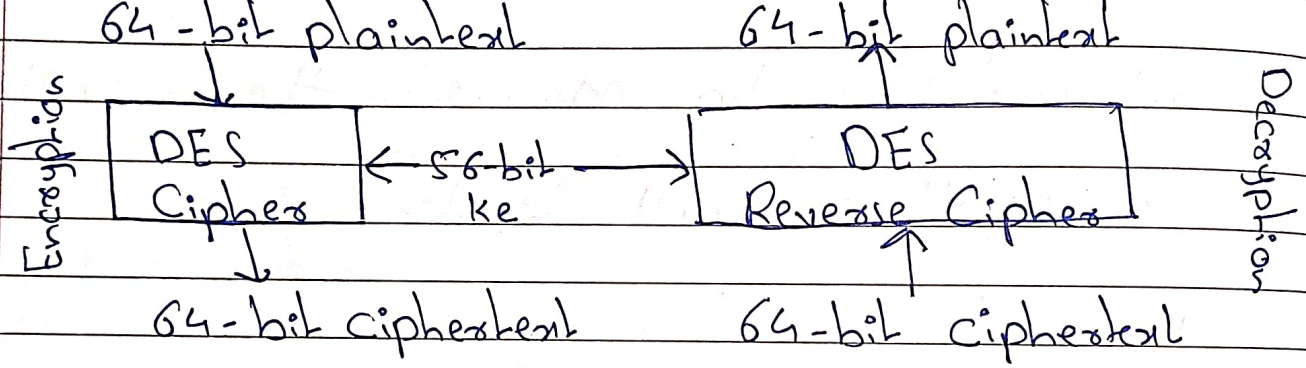
Mod 3.

DES [Data Encryption Standard].

→ Symmetric Block Cipher.
→ Input size : 64 bit
→ Output size : 64 bit
→ Main key : 64 bit
→ Subkey size : 56 bit
→ Round key size : 48 bit
→ No. of Rounds : 16 Rounds.



Steps in One Round of DES.

Step 1: Expansion (E-box) : Expand 32-bit R_i to 48-bit using an expansion table.
Step 2: Key Mixing: XOR expanded R_i with 48 bit Subkey
Step 3: Substitution (S-Box): Divide into 8 Block (6 bit each) Replace using S-Boxes Reducing 4 bit per block
Step 4: Permutation (P-Box): Rearrange 32-Bit output from S-Box using fixed permutation table
Step 5: XOR with left Half: XOR permuted Result with L_i to get new R_{i+1}
Step 6: Swap Halves : R_i become L_{i+1} and new R_{i+1} is used for the next Round.

Strength of DES.

→ Feistel structure - Allows the same process for encryption and decryption.
→ Strong Confusion and Diffusion - Uses S-Boxes and P-Boxes to scramble data.
→ Widely analyzed - One of the most studied encryption algorithm.

Weaknesses of DES.

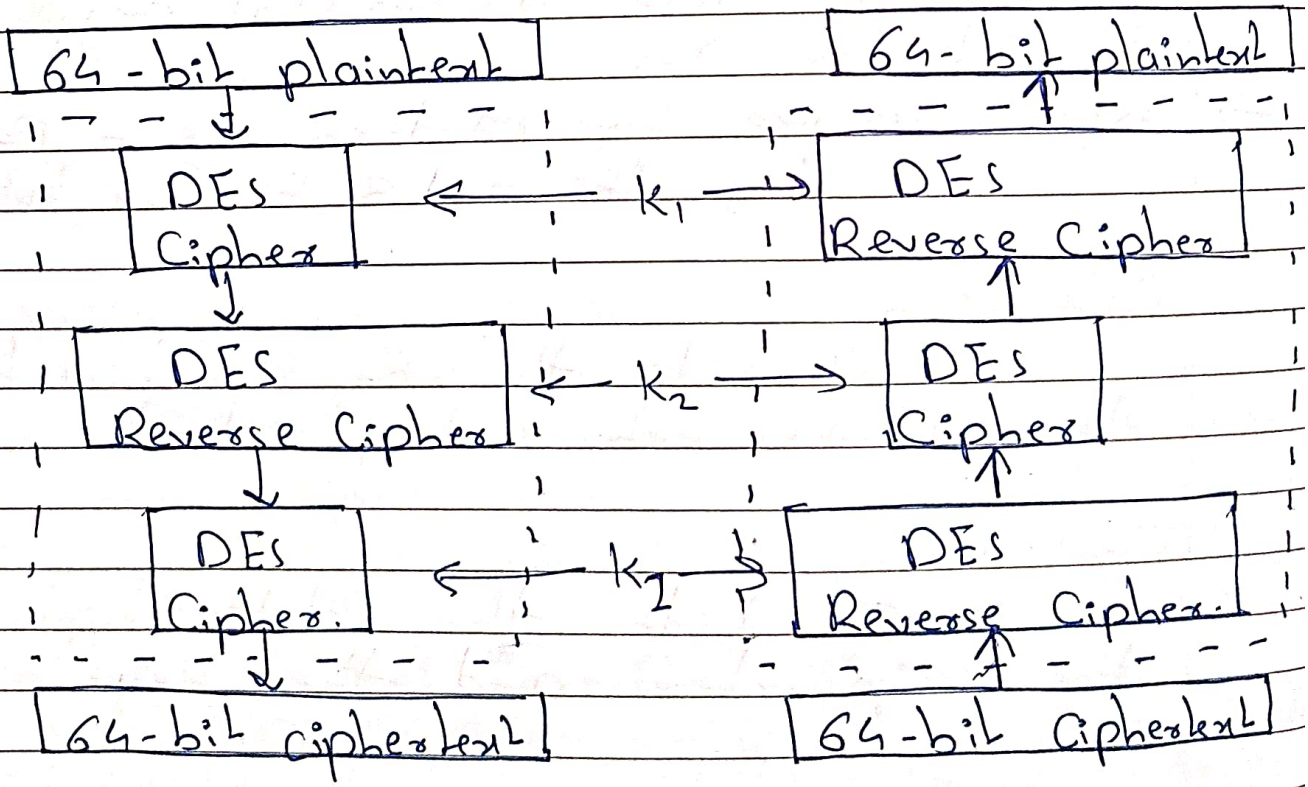
→ Small key size (56-Bit) - Vulnerable to Brute-force attack.
→ Vulnerable to Differential & Linear Cryptanalysis - Attack like differential cryptanalysis can break DES
→ Not Secure for Modern use - Replaced by AES and 3DES for better security

Diffusion
↳ It hides the Relationship between the ciphertext and plaintext.

Confusion
↳ It hides the Relationship between the ciphertext and the key.

AES	DES
Key Size: 128, 192, 256 bit	56 bit
Block Size : 128 bit	Block size : 64 bit
Round : 10	Round : 16
Structure : Substitution Permutation Network	& Feistal Network
Security : Stronger	Security : weak

Triple DES.



How Triple DES works.?

Encryption : First, encrypt the plaintext using DES with key K_1.

Decryption: Decrypt the DES with key K_2.

Encryption Again : Encrypt the Result using DES with key K_1.

Strength of 3DES.

Stronger than DES - Protects against Brute Force attack.

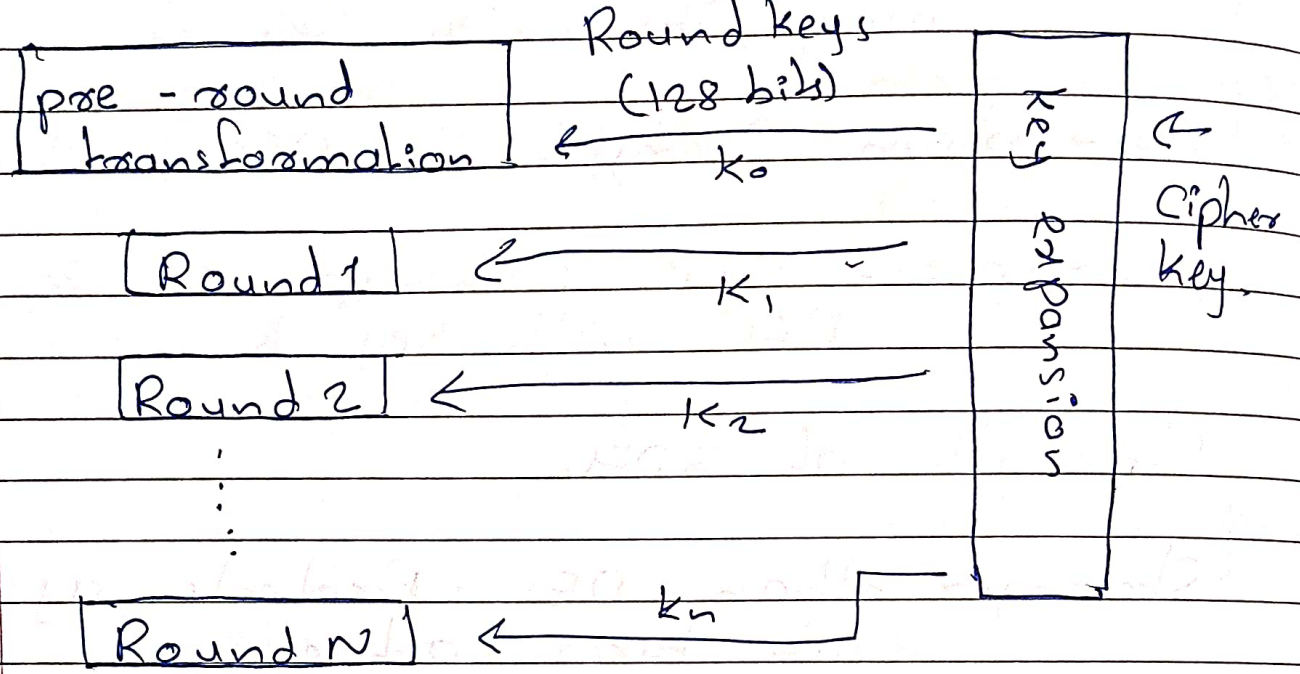
Backward Compatible - works with DES-based System.

Weaknesses of 3 DES.

Slow - Triple processing makes it inefficient compared to AES.

Vulnerable to meet-in-the-middle Attack - Still not as strong as modern encryption.

AES [Advanced Encryption Standard].



Block size : 128 Bit
Key size : 128, 192, 256 Bits
Rounds : 10 Round → 128 bit keys
12 Round → 192 bit keys
14 Round → 256 bit keys

AES Encryption Process.

1] Key Expansion
↳ The secret key is expanded into multiple rounds keys using Rijndael key schedule.

2] Initial Round.
↳ AddRoundkey : XOR plaintext with the the first Round key.

3] Main Rounds (10/12/14 Rounds).
↳ Each Round consists of :
1. SubBytes : Each byte is Replaced using S-Box.
2. ShiftRows : Bytes in each Row shifted left to mix columns.
3. Mix Columns : Matrix multiplication in GF (2^8) to spread influence.
4 AddRoundkey : XOR with Round key.

4] Final Round
↳ Subbytes, Shift Rows, AddRoundkey. (No mixcolumns)
↳ The Final Ciphertext is produced.

Strengths	Weakness
→ Highly secure	→ Vulnurable to side-channel Attacks
→ Fast & efficient	→ Future Quantum Computer may break AES-128.
→ widely used	