Introduction

The Data Encryption Standard (DES) is a symmetric-key block cipher that encrypts and decrypts data in 64-bit blocks using a 56-bit key. This report explains the complete DES encryption process, including key generation, initial permutation, 16 Feistel rounds, and the production of the final ciphertext. Furthermore, it describes how the DES decryption method is used to convert ciphertext back into plaintext by using the same key and reversing the encryption process. The code follows the official DES standard, utilizing predefined permutation tables (IP, FP, E, P, PC-1, PC-2) and S-boxes, along with custom-written functions for implementing DES manually.

Overview

The Data Encryption Standard (DES) operates through 3 main phases:

1. Key scheduling: Generates a 48-bit key from the original 64-bit key

2. Data Encryption: Processes the plaintext through initial permutation, 16 Feistel rounds, Final permutation, and Outputs ciphertext and key in hexadecimal format

3. Data Decryption: Processes the ciphertext by reversing encryption using the same key and outputs decrypted text in the original format

```
1
2   #Start with 64-bit key
3   #Pc-1 Permutation
4   #Split into 28 bits , 28 bits
5   #16 rounds of left shifts
6   #Pc-2 Permutation
7
8   #Convert plaintext to binary
9   #Apply initial permutation
10  #Divide it into 2 L and R
11  #Using 16 rounds of Feistel function (F-function)
12  #Expansion: The right half (R) is expanded from 32 bits to 48 bits using an Expansion Permutation (E-table).
13  #XOR with Key: The expanded R is XORed with a subkey derived from the original key. This results in a new 48-bit value.
14  #SBox (substitution): This 48-bit value is then passed through 8 S-boxes, each of which reduces the value back to 32 bits.
15  #Permutation (P-table)==> permuted output Xor with L ==> new R
16  #Swap L and R
17  #Final Permutation
18
19  #Output Cihpertext(Hex)
20  #Output Keytext (Hex)
21
```

Figure 1- Code Overview