DES

Supervisor : Dr. Narendran Rajagopalan, Associate Professor, NITPY

Assignment by,
M Prem Sainadh (CS22B1027)

1. Introduction:

• S-Boxes: There are 8 different S-boxes used in the DES algorithm to perform substitution on the input data. The Data Encryption Standard (DES) is a symmetric-key block cipher that was widely used for securing sensitive data. It uses a 56-bit key and processes data in 64-bit blocks. DES operates through a series of transformations and substitutions, using operations such as permutations, bit shifts, and S-box lookups, to ensure the security of the data being encrypted or decrypted. This report presents an implementation of the DES algorithm in C. The provided code demonstrates both encryption and decryption processes, as well as the necessary key schedule for each round.

2. Overview of DES Algorithm:

DES operates using several key operations: • Initial Permutation (IP): A specific permutation of the input data. • Round Function: A function that uses a round key and the data to be encrypted, involving expansion, substitution (through S-boxes), and permutation. • Key Schedule: A process to generate 16 round keys from the original key using permutation and shifting operations. • Final Permutation (PI): The inverse of the initial permutation, applied to the result to obtain the final encrypted or decrypted data.

3. Code Explanation:

The code consists of several key components: • Permutations: o IP (Initial Permutation) o PI (Inverse Initial Permutation) o E (Expansion) o P (Post S-Box permutation) o PC1 (Permuted Choice 1) o PC2 (Permuted Choice 2) • Key Schedule: The PC1 table is used to rearrange the bits of the key, followed by left shifts to generate round keys using the PC2 table. • Rounds: The algorithm performs 16 rounds of encryption/decryption, applying the round keys in each iteration.

4. Testing the Implementation:

In the provided test scenario, the encryption and decryption functions are tested for multiple rounds. The test input is: • Input (X0): 9474B8E8C73BCA7D • Final Output (X16): 1B1A2DDB4C642438 Each iteration of encryption ('e') and decryption ('d') is printed to the console, showing the intermediate results for verification.

5. Conclusion:

This implementation successfully demonstrates the DES algorithm, including the encryption, decryption, and key generation steps. The code accurately follows the DES standards as defined by FIPS PUB 46-3, allowing for the correct encryption and decryption of data.