Course CS549 Assignment 1

Implementation of the DES algorithm

Sreeparna Das (226101004)
Vishal Kumar (226101005)
Akash Lal Dutta (226101001)

February 19, 2023

Contents

List of Tables

List of Figures

The DES Algorithm : Introduction

The Data Encryption Standard (DES) algorithm is a symmetric-key block cipher used for encrypting and decrypting digital data. It takes a 64-bit block of plain-text and a 64-bit key as inputs, and produces a 64-bit block of cipher-text as output.

The algorithm consists of 16 rounds, each using a different 48-bit sub-key generated from the original 64-bit key. In each round, the 64-bit plain-text is first split into two 32-bit halves, and then a function is applied to one half using the sub-key. The result is XOR-ed with the other half, and the two halves are swapped before moving on to the next round.

The function applied in each round includes an expansion permutation, which expands the 32-bit input into a 48-bit value, and a substitution step, which replaces the 48-bit value with a different 32-bit value using a set of predefined substitution boxes. The output of the substitution step is then subjected to a permutation, known as the P-box permutation, before being XOR-ed with the other half.

After all 16 rounds have been completed, the final 64-bit output is subjected to a final permutation, which shuffles the bits according to a predetermined pattern to produce the final cipher-text.

The same algorithm and key are used for encryption and decryption, the only difference being the order in which the sub-keys are used in the rounds.

1 Structure of a key in DES Algorithm

The key in the DES algorithm is a 64-bit value used to encrypt and decrypt data. The key undergoes transformation and permutation during the key generation process to create 16 sub-keys, one for each of the 16 rounds of the DES algorithm. Each sub-key is a 48-bit value used to modify the plain-text during each round of encryption or decryption. The sub-keys are generated from the original 64-bit key through permutation, shifting, and compression.

The DES algorithm uses a technique known as the Feistel network, which means that the data is divided into two halves, left and right, and each half undergoes a series of modifications using the sub-keys. The left and right halves are swapped after each round, and the modifications are repeated. The sub-keys are generated using a combination of the original key and the results of the previous round of modifications.

The key plays a crucial role in the DES algorithm, as it determines the encryption and decryption process. To ensure the security of the data, it is important to choose a strong and unique key. However, the DES algorithm has since been replaced by more secure encryption algorithms such as AES.

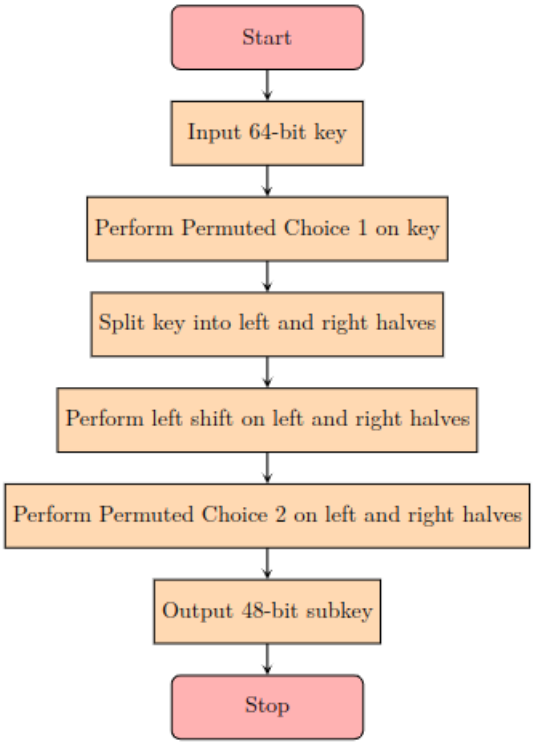

Figure 1: Flowchart of the Key Generation

2 Implementation of DES Algorithm

1. **Key Generation:** The 64-bit key can be input as a string of hexadecimal characters and converted to a binary string. The key generation algorithm can then be implemented to produce 16 round sub-keys of 48-bits each.

2. **Initial Permutation:** The 64-bit plain-text can also be input as a string of hexadecimal characters and converted to a binary string. The initial permutation algorithm can then be implemented to rearrange the bits according to a fixed permutation table.

3. **Round Function:** The 64-bit plain-text can be divided into 32-bit blocks (LPT and RPT) using slicing. Each round can then consist of the following steps:

   (a) Expansion Permutation: The RPT block can be expanded from 32-bits to 48-bits using a fixed permutation table.

   (b) Subkey Mixing: The expanded RPT block can be XORed with the corresponding 48-bit subkey for that round. The subkeys can be generated by selecting the appropriate 48-bits from the round subkeys produced in the key generation step.

   (c) S-Box Substitution: The resulting 48-bit block can then be divided into 8 6-bit blocks, each of which is substituted using a fixed S-box. The S-boxes can be implemented using lookup tables.

(d) Permutation: The resulting 32-bit block can be rearranged using a fixed permutation table.

(e) LPT and RPT Update: The resulting 32-bit block can be XORed with the LPT block, and the RPT block becomes the new LPT block.

4. **Final Permutation:** After the 16 rounds are completed, the LPT and RPT can be swapped and then subjected to a final permutation using a fixed permutation table to produce the 64-bit ciphertext.

The output of each step in the DES algorithm, including the LPT and RPT after each round and the ciphertext, can be printed or stored in variables for further analysis.

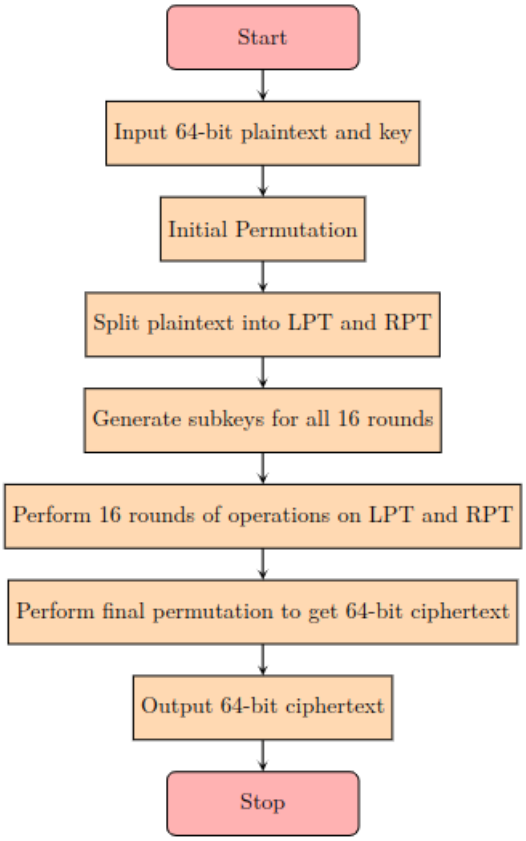

Figure 2: DES Algorithm

3 Assignment Overview

In our case, the 64-bit plain-text is formed using the last eight digits of two students' roll numbers, and the 64-bit key is formed using the last eight digits of two other students' roll numbers. The output of each step in the DES algorithm, including the **LPT** and **RPT** after each round and the cipher-text, should be documented for the given input.

3.1 Results to be produced

1. Initial permutation (mention LPT and RPT)
2. For all 16 rounds:
   (a) Expansion permutation
   (b) Sub-key used in the round
   (c) LPT and RPT after the round
3. Final permutation (mention Cipher-text)

3.2 Given Data

Student Name	**Roll Number**
Sreeparna Das	26101004
Vishal Kumar	26101005
Akash Lal Dutta	26101001
Dummy Name	26101006

Table 1: Student Information

Roll numbers in binary

Student S1 roll number = 0010 0110 0001 0000 0001 0000 0000 0100

Student S2 roll number = 0010 0110 0001 0000 0001 0000 0000 1001

Student S3 roll number = 0010 0110 0001 0000 0001 0000 0000 0001

Student S4 roll number = 0010 0110 0001 0000 0001 0000 0000 0110

For student S1 :

Plain Text	Key
S1 S2	**S3 S4**

Table 2: Plain-Text and Key for S1

3.3 Encryption

Initial Permutation

LPT	RPT
0000 0000 0110 0110 1001 1001 1000 0000	0000 0000 0001 0001 0000 0000 0001 0001

Table 3: LPT and RPT Values

Round	LPT	RPT
1	0000 0000 0001 0001 0000 0000 0001 0001	0101 0101 0010 1110 0100 0100 0001 1101
2	0101 0101 0010 1110 0100 0100 0001 1101	0010 1100 1010 0000 0001 0011 1010 0011
3	0010 1100 1010 0000 0001 0011 1010 0011	1000 1010 1010 1000 0100 1100 0100 1000
4	1000 1010 1010 1000 0100 1100 0100 1000	0111 0011 0001 1101 1011 0101 0100 0000
5	0111 0011 0001 1101 1011 0101 0101 0000	1111 1010 0110 0001 0000 1000 0000 1000
6	1111 1010 0110 0001 0000 1000 0000 1000	0011 0101 0101 1100 0110 0010 1100 1111
7	0011 0101 0101 1100 0110 0010 1100 1111	0010 1011 0111 1100 0001 1100 1011 0110
8	0010 1011 0111 1100 0001 1100 1011 0110	0010 1110 0010 1100 1110 0100 1100 1101
9	0010 1110 0010 1100 1110 0100 1100 1101	1010 0010 0100 1001 0111 0110 0000 0010
10	1010 0010 0100 1001 0111 0110 0000 0010	1100 0010 0011 0100 0101 1110 1010 1001
11	1100 0010 0011 0100 0101 1110 1010 1001	0010 0111 0110 0101 0110 0011 1000 1010
12	0010 0111 0110 0101 0110 0011 1000 1010	0101 1101 0010 0110 1110 1000 1111 1110
13	0101 1101 0010 0110 1110 1000 1111 1110	0011 1001 1110 0000 1100 0000 0000 0010
14	0011 1001 1110 0000 1100 0000 0000 0010	0001 0111 0001 0110 0100 1110 1110 0001
15	0001 0111 0001 0110 0100 1110 1110 0001	1101 1011 1111 0111 1100 0000 1100 0100
16	1101 1011 1111 0111 1100 0000 1100 0100	1101 1011 1111 0111 1100 0000 1100 0100

Table 4: Operations for all 16 Rounds

Binary Key
0010 0110 0001 0000 0001 0000 0000 0001 0010 0110 0001 0000 0001 0000 0000 0110

Table 5: Key for S1

Sub-Key
0000 0000 0000 0000 0001 0001 0110 1001 0001 1001 0001 0000 0000 0110

Table 6: PC-1 Key for S1

Round	Sub-Key
1	0000 0000 0000 1100 1000 0000 0010 0000 0000 0011 0100 0100
2	0001 0000 0000 0000 0000 0000 0100 0110 0000 0000 1101 0000
3	0000 0000 0000 1000 0010 0100 0000 0001 1010 0001 0100 1101
4	1000 0000 0010 0000 0000 0100 0010 0010 1001 0100 1000 0000
5	0000 0000 0000 0110 0010 0000 0100 1000 0000 0101 0010 0111
6	1100 0000 0001 0000 0010 0000 0000 1110 0100 1000 1000 1000
7	1000 0000 1000 0010 0100 0000 0100 0000 0101 0001 0101 0001
8	0000 0000 0101 0010 0000 0010 1000 0011 1000 0000 0010 1000
9	0010 0100 0000 0010 0000 0000 0000 0001 0100 0110 0101 1010
10	0000 0010 0001 0000 0001 0000 0001 1101 1001 0000 0000 0000
11	0000 1100 0000 0000 0101 0000 1000 0000 0100 0100 0110 0100
12	0000 0110 0100 0000 0000 1000 0000 1000 1010 1010 1000 0100
13	0000 1010 0000 0001 0000 0000 1011 0000 0100 0100 1001 0001
14	0000 1000 0000 1000 0000 1001 0000 1011 0000 0010 0000 0011
15	0000 0001 0010 0000 0000 1000 1001 0110 0110 0001 0000 0000
16	0001 0000 0000 0000 1000 1100 0001 0101 0000 1000 0000 0111

Table 7: Sub-Key Generated Table

Cipher Text
1111 0101 1111 0100 0110 0111 1001 0001 1111 0111 0001 1011 1110 1111 1011

Table 8: Cipher Text Generated

LPT	RPT
1011 0111 1111 1011 0101 0111 1011 1101	1101 1011 1111 0111 1100 0000 1100 0100

Table 9: LPT and RPT Values

Round	LPT	RPT
1	1101 1011 1111 0111 1100 0000 1100 0100	0001 0111 0001 0110 0100 1110 1110 0001
2	0001 0111 0001 0110 0100 1110 1110 0001	0011 1001 1110 0000 1100 0000 0000 0010
3	0011 1001 1110 0000 1100 0000 0000 0010	0101 1101 0010 0110 1110 1000 1111 1110
4	0101 1101 0010 0110 1110 1000 1111 1110	0010 0111 0110 0101 0110 0011 1000 1010
5	0010 0111 0110 0101 0110 0011 1000 1010	1100 0010 0011 0100 0101 1110 1010 1001
6	1100 0010 0011 0100 0101 1110 1010 1001	1010 0010 0100 1001 0111 0110 0000 0010
7	1010 0010 0100 1001 0111 0110 0000 0010	0010 1110 0010 1100 1110 0100 1100 1101
8	0010 1110 0010 1100 1110 0100 1100 1101	0010 1011 0111 1100 0001 1100 1011 0110
9	0010 1011 0111 1100 0001 1100 1011 0110	0011 0101 0101 1100 0110 0010 1100 1111
10	0011 0101 0101 1100 0110 0010 1100 1111	1111 1010 0110 0001 0000 1000 0000 1000
11	1111 1010 0110 0001 0000 1000 0000 1000	0111 0011 0001 1011 0101 0100 0101 0000
12	0111 0011 0001 1011 0101 0100 0101 0000	1000 0110 1010 1000 0100 1100 0100 1000
13	1000 0110 1010 1000 0100 1100 0100 1000	0010 1100 1010 0000 0001 0011 1010 0011
14	0010 1100 1010 0000 0001 0011 1010 0011	0101 0101 0010 1110 0100 0100 0001 1101
15	0101 0101 0010 1110 0100 0100 0001 1101	0000 0000 0001 0001 0000 0000 0001 0001
16	0000 0000 0110 0110 1001 1001 1000 0000	0000 0000 0001 0001 0000 0000 0001 0001

Table 10: Operations for all 16 Rounds of Decryption

Binary Key
0010 0110 0001 0000 0001 0000 0000 0001 0010 0110 0001 0000 0001 0000 0000 0110

Table 11: Key for S1

Sub-Key
0000 0000 0000 0000 0001 0001 0110 1001 0001 1001 0001 0000 0000 0110

Table 12: PC-1 Key for S1

Round	Sub-Key
1	0001 0000 0000 0000 1000 1100 0001 0101 0000 1000 0000 0111
2	0000 0001 0010 0000 0000 1000 1001 0110 0110 0001 0000 0000
3	0000 1000 0000 1000 0000 1001 0000 1011 0000 0010 0000 0011
4	0000 1010 0000 0001 0000 0000 1011 0000 0100 0100 1001 0001
5	0000 0110 0100 0000 0000 1000 0000 1000 1010 1010 1000 0100
6	0000 1100 0000 0000 0101 0000 1000 0000 0100 0100 0110 0100
7	0000 0010 0001 0000 0001 0000 0001 1101 1001 0000 0000 0000
8	0010 0100 0000 0010 0000 0000 0000 0001 0100 0110 0101 1010
9	0000 0000 0101 0010 0000 0010 1000 0011 1000 0000 0010 1000
10	1000 0000 1000 0010 0100 0000 0100 0000 0101 0001 0101 0001
11	1100 0000 0001 0000 0010 0000 0000 1110 0100 1000 1000 1000
12	0000 0000 0000 0110 0010 0000 0100 1000 0000 0101 0010 0111
13	1000 0000 0010 0000 0000 0100 0010 0010 1001 0100 1000 0000
14	0000 0000 0000 1000 0010 0100 0000 0001 1010 0001 0100 1101
15	0001 0000 0000 0000 0000 0000 0100 0110 0000 0000 1101 0000
16	0000 0000 0000 1100 1000 0000 0010 0000 0000 0011 0100 0100

Table 13: Sub-Key Generated Table for Decryption

Plain Text
010 0110 0001 0000 0001 0000 0000 0100 010 0110 0001 0000 0001 0000 0000 1001

Table 14: Plain Text Generated