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.

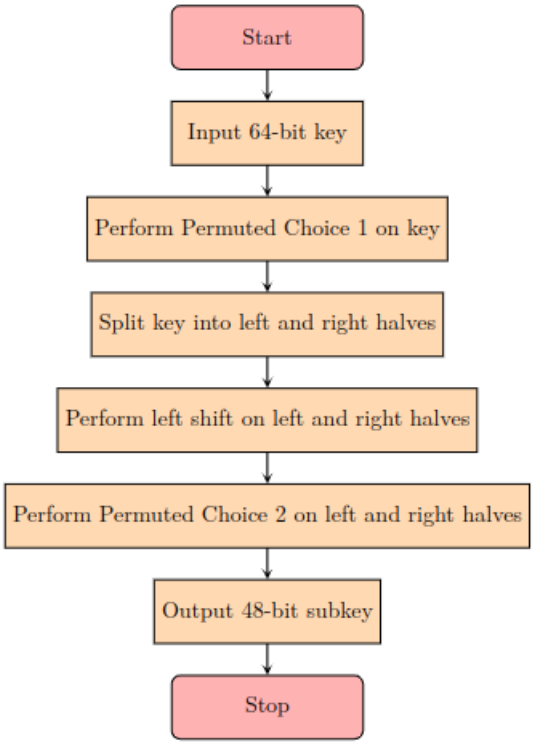

Figure 1: Flowchart of the Key Generation

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.

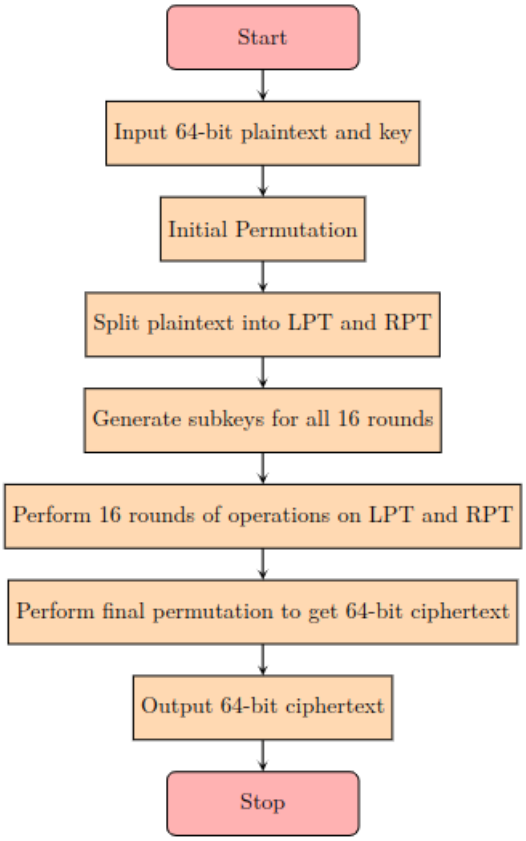

Figure 2: DES Algorithm

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

3.3 For student S1 :

Plain Text	Key
S1 S2	**S3 S4**

Table 2: Plain-Text and Key for S1

Initial Permutation

LPT	RPT
00669980	00110011

Table 3: LPT and RPT Values

Round	Exapansion Permutation
1	8000A28000A2
2	AAA95C2080FA
3	9595000A7D06
4	40D550258251
5	3A68FBDAAAA0
6	7F4302850051
7	9AAAF830565E
8	156BF80F95AC
9	95C15970965A
10	504252BAC005
11	E041A82FD553
12	10EB0AB07C54
13	2FA90D7517FC
14	1F3F01600004
15	8AE8AC25D702
16	6F7FAFE01609

Table 4: Expansion Permutation

Round	LPT	RPT
1	00110011	552E441D
2	552E441D	2CA013A3
3	2CA013A3	86A84C48
4	86A84C48	731DB550
5	731DB550	FA610808
6	FA610808	355C62CF
7	355C62CF	2B7C1CB6
8	2B7C1CB6	2E2CE4CD
9	2E2CE4CD	A2497602
10	A2497602	C2345EA9
11	C2345EA9	2765638A
12	2765638A	5D26E8FE
13	5D26E8FE	39E0C002
14	39E0C002	17164EE1
15	17164EE1	DBF7C0C4
16	DBF7C0C4	B7FB57BD

Table 5: LPT and RPT values after each of 16 Rounds

Round	Sub-Key
1	000C80200344
2	1000004600D0
3	00082401A14D
4	802004229480
5	000620480527
6	C010200E4888
7	808240405151
8	005202838028
9	24020001465A
10	0210101D9000
11	0C0050804464
12	06400808AA84
13	0A0100B04491
14	0808090B0203
15	012008966100
16	10008C150807

Table 6: Sub-Key values after each of 16 rounds

Cipher Text
FAF89B62FAB27DF7

Table 7: Cipher Text Generated

3.4 For student S2 :

Plain Text	Key
S2 S3	**S4 S1**

Table 8: Plain-Text and Key for S2

Initial Permutation

LPT	RPT
00661988	00110011

Table 9: LPT and RPT Values

Round	Exapansion Permutation
1	8000A28000A2
2	A0E95D6000FA
3	0FC2001AFF00
4	C0D454306BAF
5	F0AA581FBEFF
6	B0FD0FDAFFFA
7	7A83540FA905
8	357D0BDA54F8
9	45FD5BF515F9
10	A03FA6BA5706
11	EF02082F0207
12	E595AA9A80FB
13	D581FAA043FB
14	EF03517A40A3
15	9AFEF680BC5A
16	40D7A7E5D501

Table 10: Expansion Permutation

Round	LPT	RPT
1	00110011	472EC01D
2	472EC01D	1E4037E0
3	1E4037E0	868A6377
4	868A6377	E54C3DDF
5	E54C3DDF	67A7B7FD
6	67A7B7FD	F46A1D22
7	F46A1D22	6BA5B29C
8	6BA5B29C	8FADE8BC
9	8FADE8BC	41F372E3
10	41F372E3	D8445843
11	D8445843	CCB5341D
12	CCB5341D	AC3D427D
13	AC3D427D	D868F211
14	D868F211	37DB058D
15	37DB058D	86F3CEA0
16	86F3CEA0	9EC7A381

Table 11: LPT and RPT values after each of 16 Rounds

Round	**Sub-Key**
1	000C80210241
2	1000006202D0
3	00082411810F
4	802004061480
5	000620482165
6	C0102022C888
7	808240401513
8	0052028F0028
9	240200014662
10	0210105C8800
11	0C005080445C
12	06400809B280
13	0A0100B04421
14	0808090A0A06
15	012008946190
16	10008C852805

Table 12: Sub-Key values after each of 16 rounds

Cipher Text
3AFCE484901934FF

Table 13: Cipher Text Generated

3.5 For student S3 :

Plain Text	Key
S3 S4	**S2 S1**

Table 14: Plain-Text and Key for S3

Initial Permutation

LPT	RPT
00669108	00110091

Table 15: LPT and RPT Values

Round	Exapansion Permutation
1	8000A28014A2
2	A0E8FC2594AA
3	9001A685EA5A
4	4F55A14A7E09
5	9FD4F0152AA6
6	AF7D53CFAAAA
7	209557CA9608
8	0A6856A5BDA4
9	B594081F8002
10	20D45BE5545C
11	70BEF82543F9
12	10805FEF7F54
13	FA170FDA3D5F
14	FA42FA8F570B
15	CFBFAAB081AB
16	5094F0209605

Table 16: Expansion Permutation

Round	LPT	RPT
1	00110091	471E4C95
2	471E4C95	20330F4D
3	20330F4D	9AB093C4
4	9AB093C4	3E982953
5	3E982953	5BA99D55
6	5BA99D55	44AB94C4
7	44AB94C4	130B4DB2
8	130B4DB2	6C843C01
9	6C843C01	468DCA8E
10	468DCA8E	E5DC4A7C
11	E5DC4A7C	240FDBEA
12	240FDBEA	F0E7B1AF
13	F0E7B1AF	F25D1AE5
14	F25D1AE5	9DF56435
15	9DF56435	A49844C2
16	A49844C2	D5FD2EC3

Table 17: LPT and RPT values after each of 16 Rounds

Round	**Sub-Key**
1	000C80210244
2	1000004202D0
3	00082411A10D
4	802004229480
5	000620482127
6	C01020264888
7	808240401153
8	005202878028
9	24020001464A
10	0210105C9000
11	0C005080446C
12	06400808BA80
13	0A0100B04431
14	0808090B0A02
15	012008946110
16	10008C950805

Table 18: Sub-Key values after each of 16 rounds

Cipher Text
A20BEC38B068A7F3

Table 19: Cipher Text Generated

3.6 For student S4 :

Plain Text	Key
S4 S1	**S3 S2**

Table 20: Plain-Text and Key for S4

Initial Permutation

LPT	RPT
00669900	00110019

Table 21: LPT and RPT Values

Round	Exapansion Permutation
1	8000A28000F2
2	2FA95C2015F8
3	35E8A82F28A4
4	DFFCA56002FF
5	5056FC2AE851
6	4A150EBF4355
7	153E5EA54254
8	85AB5E807C0E
9	9FAA5D5ABEA2
10	3A5556BFAA58
11	D5550FDFABF3
12	7FFC515A7C0D
13	0F54582A7EA4
14	2A1753EFEA0C
15	053C0805280C
16	DFD457D04207

Table 22: Expansion Permutation

Round	LPT	RPT
1	00110019	5D2E40BC
2	5D2E40BC	6F145912
3	6F145912	BF92C05F
4	BF92C05F	A2DE5708
5	A2DE5708	90A77A6A
6	90A77A6A	29CF4A4A
7	29CF4A4A	0D6F0387
8	0D6F0387	3D4EB5D1
9	3D4EB5D1	72AB7D4C
10	72AB7D4C	AAA7BD79
11	AAA7BD79	FF88B386
12	FF88B386	1A8C53D2
13	1A8C53D2	50E9DF46
14	50E9DF46	09840906
15	09840906	BE8BA243
16	BE8BA243	497A2AD5

Table 23: LPT and RPT values after each of 16 Rounds

Round	**Sub-Key**
1	000C80200244
2	1000004200D0
3	00082401A10D
4	802004221480
5	000620480127
6	C01020064888
7	808240401151
8	005202838028
9	24020001464A
10	0210101C9000
11	0C0050804464
12	06400808AA80
13	0A0100B04411
14	0808090B0202
15	012008946100
16	10008C150805

Table 24: Sub-Key values after each of 16 rounds

Cipher Text
937D42F8626CA356

Table 25: Cipher Text Generated