CS549: Computer and Network Security Assignment 1

Group-6
Rishav Mondal (190101072)
Siddharth Charan(190101085)
Raahil Badiani (190101068)
Yashwardhan Modi (190101101)

February 19, 2023

1 Question

In this assignment, we were told to run the DES algorithm and write details of all intermediate steps for 4 different choices of plaintext and key derived from the roll numbers of the 4 members of the group. From here on, we use the notation S_1, S_2, S_3, S_4 to mean the last 8 digits of the roll number for each group member, where each digit is represented as hexadecimal:

- S_1 : 90101072
- S_2 : 90101085
- S_3 : 90101068
- S_4 : 90101101

2 For student S_1

In this case, the choice for plaintext and key are as follows:

Plaintext : S_1S_2 = 9010 1072 9010 1085
Key : S_3S_4 = 9010 1068 9010 1101

where each digit is represented as hexadecimal. We obtain the following output:

- Initial permutation: 087F808091080008
- Initial permutation after splitting into LPT and RPT : LPT0=087F8080 RPT0=91080008
- Round 1 Expansion Permutation 4A2850000051
- Round 1 Subkey Used 02029C041040
- Round 1 LPT1 = 91080008, RPT1 = 95CBC360
- Round 2 Expansion Permutation 4ABE57E06B01
- Round 2 Subkey Used 304481480040
- Round 2 LPT2 = 95CBC360, RPT2 = 642CBF03
- Round 3 Expansion Permutation B081595FE806
- Round 3 Subkey Used 51090040C008
- Round 3 LPT3 = 642CBF03, RPT3 = 12C7C972
- Round 4 Expansion Permutation 0A560FE52BA4
- Round 4 Subkey Used 00A095001408
- Round 4 LPT4 = 12C7C972, RPT4 = 2D2F0BE3

- Round 5 Expansion Permutation 95A95E857F06
- Round 5 Subkey Used 150406881020
- Round 5 LPT5 = 2D2F0BE3, RPT5 = F18E00BF
- Round 6 Expansion Permutation FA3C5C0015FF
- Round 6 Subkey Used 6200A0004A20
- Round 6 LPT6 = F18E00BF, RPT6 = 29B44A3E
- Round 7 Expansion Permutation 153DA82541FC
- Round 7 Subkey Used 988024100810
- Round 7 LPT7 = 29B44A3E, RPT7 = 5821E1DE
- Round 8 Expansion Permutation 2F0103F03EFC
- Round 8 Subkey Used 80021A810010
- Round 8 LPT8 = 5821E1DE, RPT8 = A4332F88
- Round 9 Expansion Permutation 5081A695FC51
- Round 9 Subkey Used 606282810280
- Round 9 LPT9 = A4332F88, RPT9 = D4A0C620
- Round 10 Expansion Permutation 6A950160C101
- Round 10 Subkey Used 309500100201
- Round 10 LPT10 = D4A0C620, RPT10 = 2D97B665
- Round 11 Expansion Permutation 95BCAFDAC30A
- Round 11 Subkey Used 400053120004
- Round 11 LPT11 = 2D97B665, RPT11 = F1898D6F
- Round 12 Expansion Permutation FA3C53C5AB5F
- Round 12 Subkey Used 25C014002180
- Round 12 LPT12 = F1898D6F, RPT12 = BD2864ED
- Round 13 Expansion Permutation DFA95030975B
- Round 13 Subkey Used 060182202001
- Round 13 LPT13 = BD2864ED, RPT13 = E1CD0E60
- Round 14 Expansion Permutation 703E5A85C301
- Round 14 Subkey Used 3A0031620002
- Round 14 LPT14 = E1CD0E60, RPT14 = 20824F48
- Round 15 Expansion Permutation 10140425EA50
- Round 15 Subkey Used 8D000804010A
- Round 15 LPT15 = 20824F48, RPT15 = 55E128B1
- Round 16 Expansion Permutation AABF029515A2
- Round 16 Subkey Used 0121CA040500
- Round 16 LPT16 = 0EA1C141, RPT16 = 55E128B1

Final Permutation (Ciphertext) : B740C048823AA536

3 For student S_2

In this case, the choice for plaintext and key are as follows:

Plaintext : S_2S_3 = 9010 1085 9010 1068
Key : S_4S_1 = 9010 1101 9010 1072

where each digit is represented as hexadecimal. We obtain the following output:

- Initial permutation: 8077080819808000
- Initial permutation after splitting into LPT and RPT : LPT0=80770808 RPT0=19808000
- Round 1 Expansion Permutation 0F3C01400000
- Round 1 Subkey Used 1200F8040140
- Round 1 LPT1 = 19808000, RPT1 = BE729565
- Round 2 Expansion Permutation DFC3A54AAB0B
- Round 2 Subkey Used 10C891440040
- Round 2 LPT2 = BE729565, RPT1 = AC42CE97
- Round 3 Expansion Permutation D5820565D4AF
- Round 3 Subkey Used 152902408048
- Round 3 LPT3 = AC42CE97, RPT3 = 68FC6B4B
- Round 4 Expansion Permutation B517F8356A56
- Round 4 Subkey Used 222485009408
- Round 4 LPT4 = 68FC6B4B, RPT4 = DD95C2A2
- Round 5 Expansion Permutation 6FBCABE05505
- Round 5 Subkey Used 590404081420
- Round 5 LPT5 = DD95C2A2, RPT5 = 1057AFBD
- Round 6 Expansion Permutation 8A02AFD5FDFA
- Round 6 Subkey Used 4080B8084820
- Round 6 LPT6 = 1057AFBD, RPT6 = AC2C72E7
- Round 7 Expansion Permutation D581583A570F
- Round 7 Subkey Used 948026004810
- Round 7 LPT7 = AC2C72E7, RPT7 = 1259FD36
- Round 8 Expansion Permutation 0A42F3FFA9AC
- Round 8 Subkey Used A20A02810010
- Round 8 LPT8 = 1259FD36, RPT8 = 3E30F902
- Round 9 Expansion Permutation 1FC1A17F2804
- Round 9 Subkey Used 603203810210
- Round 9 LPT9 = 3E30F902 RPT9 = 26A2A5BF
- Round 10 Expansion Permutation 90D50550BDFE
- Round 10 Subkey Used 219444110200
- Round 10 LPT10 = 26A2A5BF RPT10 = E700CB43

- Round 11 Expansion Permutation F0E801656A07
- Round 11 Subkey Used 4040D2100004
- Round 11 LPT11 = E700CB43 RPT11 = EFF8FE92
- Round 12 Expansion Permutation 75FFF17FD4A5
- Round 12 Subkey Used 34C130002084
- Round 12 LPT12 = EFF8FE92 LPT12 = 17107FD89
- Round 13 Expansion Permutation BA280FFFBC52
- Round 13 Subkey Used 860103202081
- Round 13 LPT13 = 7107FD89 RPT13 = 4CC9B6F8
- Round 14 Expansion Permutation 259653DAD7F0
- Round 14 Subkey Used 2B0215220003
- Round 14 LPT14 = 4CC9B6F8 LPT14 = A8D31B2F
- Round 15 Expansion Permutation D516A68F695F
- Round 15 Subkey Used 0D1088060102
- Round 15 LPT15 = A8D31B2F RPT15 = 80D16926
- Round 16 Expansion Permutation 4016A2B5290D
- Round 16 Subkey Used 4101C8040102
- Round 16 LPT16 = 1E1EB8D3 RPT16 = 80D16926

Final Permutation (Ciphertext) : 2953525C750E29A5

4 For student S_3

In this case, the choice for plaintext and key are as follows:

Plaintext : S_3S_4 = 9010 1068 9010 1101
Key : S_2S_1 = 9010 1085 9010 1072

where each digit is represented as hexadecimal. We obtain the following output:

- Initial permutation: 087700C011080800
- Initial permutation after splitting into LPT and RPT : LPT0=087700C0 RPT0=11080800
- Round 1 Expansion Permutation 0A2850050000
- Round 1 Subkey Used 1201F8050140
- Round 1 LPT1 = 11080800 RPT1 = 16775D2B
- Round 2 Expansion Permutation 8AC3AEAFA956
- Round 2 Subkey Used 12C891440240
- Round 2 LPT2 = 16775D2B RPT2 = 6FD27CFC
- Round 3 Expansion Permutation 35FEA43F97F8
- Round 3 Subkey Used 1D2902508048
- Round 3 LPT3 = 6FD27CFC RPT3 = 25DFFE29
- Round 4 Expansion Permutation 90BEFFFFC152

- Round 4 Subkey Used 22248D009408
- Round 4 LPT4 = 25DFFE29 RPT4 = 8DC31E78
- Round 5 Expansion Permutation 45BE068FC3F1
- Round 5 Subkey Used 590404083420
- Round 5 LPT5 = 8DC31E78 RPT5 = DCCF4BC1
- Round 6 Expansion Permutation EF965EA57E03
- Round 6 Subkey Used 4088B8284820
- Round 6 LPT6 = DCCF4BC1 RPT6 = CA5A767A
- Round 7 Expansion Permutation 6542F43AC3F5
- Round 7 Subkey Used 94A026004812
- Round 7 LPT7 = CA5A767A RPT7 = 9EB0C763
- Round 8 Expansion Permutation CFD5A160EB07
- Round 8 Subkey Used A20E02850010
- Round 8 LPT8 = 9EB0C763 RPT8 = 11208AB8
- Round 9 Expansion Permutation 0A29014555F0
- Round 9 Subkey Used 603203810210
- Round 9 LPT9 = 11208AB8 RPT9 = 1A2E9B9D
- Round 10 Expansion Permutation 8F415D4F7CFA
- Round 10 Subkey Used 219464510200
- Round 10 LPT10 = 1A2E9B9D RPT10 = 00A797E2
- Round 11 Expansion Permutation 00150FCAFF04
- Round 11 Subkey Used C040D210000C
- Round 11 LPT11 = 00A797E2 RPT11 = 28C908EA
- Round 12 Expansion Permutation 151652851754
- Round 12 Subkey Used 34C330003084
- Round 12 LPT12 = 28C908EA RPT12 = 7DFCE16A
- Round 13 Expansion Permutation 3FBFF9702B54
- Round 13 Subkey Used 8611032020A1
- Round 13 LPT13 = 7DFCE16A RPT13 = 16180660
- Round 14 Expansion Permutation 0AC0F000C300
- Round 14 Subkey Used 2B0255220803
- Round 14 LPT14 = 16180660 RPT14 = 43EAAFD6
- Round 15 Expansion Permutation 207F5555FEAC
- Round 15 Subkey Used 0D5088060112
- Round 15 LPT15 = 43EAAFD6 RPT15 = 6E5971B8
- Round 16 Expansion Permutation 35C2F2BA3DF0
- Round 16 Subkey Used 4501C8840102
- Round 16 LPT16 = 2599CEF2 RPT16 = 6E5971B8

Final Permutation (Ciphertext) : 7885C4B63BCBAD17

5 For student S_4

In this case, the choice for plaintext and key are as follows:

Plaintext : S_4S_1 = 9010 1101 9010 1072
Key : S_3S_2 = 9010 1068 9010 1085

where each digit is represented as hexadecimal. We obtain the following output:

- Initial permutation: 80F7000C11800080
- Initial permutation after splitting into LPT and RPT : LPT0=80F7000C RPT0=11800080
- Round 1 Expansion Permutation 0A3C00001400
- Round 1 Subkey Used 03029C041044
- Round 1 LPT1 11800080 RPT1 99E39581
- Round 2 Expansion Permutation CF3F07CABC03
- Round 2 Subkey Used 304489480040
- Round 2 LPT2 99E39581 RPT2 1B4EA8FB
- Round 3 Expansion Permutation 8F6A5D5517F6
- Round 3 Subkey Used 51090040E008
- Round 3 LPT3 1B4EA8FB RPT3 C13A4345
- Round 4 Expansion Permutation E029F4206A0B
- Round 4 Subkey Used 00A895201408
- Round 4 LPT4 C13A4345 RPT4 D32CA249
- Round 5 Expansion Permutation EA6959504253
- Round 5 Subkey Used 152406881022
- Round 5 LPT5 D32CA249 RPT5 69A5CA3B
- Round 6 Expansion Permutation B53D0BE541F6
- Round 6 Subkey Used 6204A0044A20
- Round 6 LPT6 69A5CA3B RPT6 1D3AA5FB
- Round 7 Expansion Permutation 8FA9F550BFF6
- Round 7 Subkey Used D88024100850
- Round 7 LPT7 1D3AA5FB RPT7 7A2D5233
- Round 8 Expansion Permutation BF415AAA41A6
- Round 8 Subkey Used 80821A818010
- Round 8 LPT8 7A2D5233 RPT8 C44B995C
- Round 9 Expansion Permutation 608257CF2AF9
- Round 9 Subkey Used E06282810288
- Round 9 LPT9 C44B995C RPT9 665EDE0F
- Round 10 Expansion Permutation B0C2FD6FC05E
- Round 10 Subkey Used 309700101201
- Round 10 LPT10 665EDE0F RPT10 D41C18C8

- Round 11 Expansion Permutation 6A80F80F1651
- Round 11 Subkey Used 401053120024
- Round 11 LPT11 D41C18C8 RPT11 AFFA1005
- Round 12 Expansion Permutation D5FFF40A000B
- Round 12 Subkey Used 25C054002980
- Round 12 LPT12 AFFA1005 RPT12 C363D097
- Round 13 Expansion Permutation E06B07EA14AF
- Round 13 Subkey Used 064182202011
- Round 13 LPT13 C363D097 RPT13 42033350
- Round 14 Expansion Permutation 2040069A6AA0
- Round 14 Subkey Used 3A0131630002
- Round 14 LPT14 42033350 RPT14 0C259D4D
- Round 15 Expansion Permutation 85810BCFAA5A
- Round 15 Subkey Used 8D000904010A
- Round 15 LPT15 0C259D4D RPT15 BF018609
- Round 16 Expansion Permutation DFE803C0C053
- Round 16 Subkey Used 0921CA140500
- Round 16 LPT16 0E5DC777 RPT16 BF018609

Final Permutation (Ciphertext) : B7CDDDD29181158C