

**AHSANULLAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

Department of Computer Science and Engineering

Program: Bachelor of Science in Computer Science and Engineering

Course Code: CSE 4174

Course Title: Cyber Security Lab

Academic Semester: Spring 2023

Assignment Topic: DES Calculator

Submitted on: 21/01/2024

Submitted by

Name: Yasir Arafah Prince

Student ID: 20200104042

Lab Section: A2

**Question:** Observe the avalanche effect of DES using the DES Calculator (DEScalc[dot]jar) from the provided link.

As the original text, use Ansary’s and as the original key, use MDAnsary. While operating the DES Calculator, for Trace level, choose 2: +rounds

**Answer:**

Ansary’s in hex: 416E736172792773

MDAnsary in hex: 4D44416E73617279

After encryption we get:

setKey(4d44416e73617279)

encryptDES(416e736172792773)

IP: L0=bfb442ed, R0=00fe22d6

Rnd1 f(R0=00fe22d6, SK1=3c 09 19 2e 08 19 20 13 ) = 6b53a99e

Rnd2 f(R1=d4e7eb73, SK2=3c 09 3b 32 2a 20 0c 18 ) = 19720882

Rnd3 f(R2=198c2a54, SK3=3d 0f 09 32 24 15 0c 02 ) = fd7104e1

Rnd4 f(R3=2996ef92, SK4=29 2d 1d 16 15 00 08 20 ) = fe5d5294

Rnd5 f(R4=e7d178c0, SK5=1b 25 0d 17 34 02 21 0c ) = b5329c3d

Rnd6 f(R5=9ca473af, SK6=0b 3d 05 39 08 0b 0a 18 ) = b818024f

Rnd7 f(R6=5fc97a8f, SK7=23 34 07 3b 0c 13 10 23 ) = 4753226d

Rnd8 f(R7=dbf751c2, SK8=2f 34 2e 19 0b 20 20 22 ) = b7fa68fa

Rnd9 f(R8=e8331275, SK9=0f 35 26 0b 04 24 06 22 ) = ff9b95c9

Rnd10 f(R9=246cc40b, SK10=0e 32 27 0d 31 00 24 01 ) = 7e13eb45

Rnd11 f(R10=9620f930, SK11=06 16 32 1d 30 22 09 18 ) = 6317df00

Rnd12 f(R11=477b1b0b, SK12=15 12 36 3c 1c 19 0c 08 ) = 3063dfb1

Rnd13 f(R12=a6432681, SK13=35 2a 32 25 04 01 10 2a ) = c07c516c

Rnd14 f(R13=87074a67, SK14=36 3a 38 26 13 03 20 24 ) = 3e3a15de

Rnd15 f(R14=9879335f, SK15=3a 0b 1a 2e 08 06 23 38 ) = 1f91f611

Rnd16 f(R15=9896bc76, SK16=38 1b 1a 26 30 26 30 01 ) = b8e734f6

FP: L=05363e99, R=ba4b02b9

returns 05363e99ba4b02b9

After converting each round into 16 bit hex value:

|  |  |
| --- | --- |
| Round | 16 bit Hex |
| 1 | 00fe22d6d4e7eb73 |
| 2 | d4e7eb73198c2a54 |
| 3 | 198c2a542996ef92 |
| 4 | 2996ef92e7d178c0 |
| 5 | e7d178c09ca473af |
| 6 | 9ca473af5fc97a8f |
| 7 | 5fc97a8fdbf751c2 |
| 8 | dbf751c2e8331275 |
| 9 | e8331275246cc40b |
| 10 | 246cc40b9620f930 |
| 11 | 9620f930477b1b0b |
| 12 | 477b1b0ba6432681 |
| 13 | a643268187074a67 |
| 14 | 87074a679879335f |
| 15 | 9879335f9896bc76 |
| 16 | 9896bc76209e07a9 |
| Result | 05363e99ba4b02b9 |

After Altered 12th position (9 -> A) in original text

Ansary’s in hex: 416E7361727**A**2773

MDAnsary in hex: 4D44416E73617279

After encryption we get:

setKey(4d44416e73617279)

encryptDES(416e7361727a2773)

IP: L0=bfb442cd, R0=00fe22f6

Rnd1 f(R0=00fe22f6, SK1=3c 09 19 2e 08 19 20 13 ) = 6943ad9e

Rnd2 f(R1=d6f7ef53, SK2=3c 09 3b 32 2a 20 0c 18 ) = 4f7359db

Rnd3 f(R2=4f8d7b2d, SK3=3d 0f 09 32 24 15 0c 02 ) = 262dfae0

Rnd4 f(R3=f0da15b3, SK4=29 2d 1d 16 15 00 08 20 ) = 49c1778e

Rnd5 f(R4=064c0ca3, SK5=1b 25 0d 17 34 02 21 0c ) = dc626920

Rnd6 f(R5=2cb87c93, SK6=0b 3d 05 39 08 0b 0a 18 ) = 4fd55312

Rnd7 f(R6=49995fb1, SK7=23 34 07 3b 0c 13 10 23 ) = 32d4da8f

Rnd8 f(R7=1e6ca61c, SK8=2f 34 2e 19 0b 20 20 22 ) = d244179d

Rnd9 f(R8=9bdd482c, SK9=0f 35 26 0b 04 24 06 22 ) = 840149ec

Rnd10 f(R9=9a6deff0, SK10=0e 32 27 0d 31 00 24 01 ) = f50b1fb7

Rnd11 f(R10=6ed6579b, SK11=06 16 32 1d 30 22 09 18 ) = f29221c2

Rnd12 f(R11=68ffce32, SK12=15 12 36 3c 1c 19 0c 08 ) = 090fc07e

Rnd13 f(R12=67d997e5, SK13=35 2a 32 25 04 01 10 2a ) = e6be3c26

Rnd14 f(R13=8e41f214, SK14=36 3a 38 26 13 03 20 24 ) = 541a4bac

Rnd15 f(R14=33c3dc49, SK15=3a 0b 1a 2e 08 06 23 38 ) = 2b6d44fc

Rnd16 f(R15=a52cb6e8, SK16=38 1b 1a 26 30 26 30 01 ) = 394b17d9

FP: L=844ca876, R=09aa069f

returns 844ca87609aa069f

Again for this converting each round into 16 bit hex value:

|  |  |
| --- | --- |
| Round | 16 bit Hex |
| 1 | 00fe22f6d6f7ef53 |
| 2 | d6f7ef534f8d7b2d |
| 3 | 4f8d7b2df0da15b3 |
| 4 | f0da15b3064c0ca3 |
| 5 | 064c0ca32cb87c93 |
| 6 | 2cb87c9349995fb1 |
| 7 | 49995fb11e6ca61c |
| 8 | 1e6ca61c9bdd482c |
| 9 | 9bdd482c9a6deff0 |
| 10 | 9a6deff06ed6579b |
| 11 | 6ed6579b68ffce32 |
| 12 | 68ffce3267d997e5 |
| 13 | 67d997e58e41f214 |
| 14 | 8e41f21433c3dc49 |
| 15 | 33c3dc49a52cb6e8 |
| 16 | a52cb6e8a88cb90 |
| Result | 844ca87609aa069f |

Now comparing the changes for each round:

|  |  |
| --- | --- |
| Round | Total Digit Changed |
| 1 | 5 |
| 2 | 17 |
| 3 | 29 |
| 4 | 33 |
| 5 | 31 |
| 6 | 27 |
| 7 | 35 |
| 8 | 41 |
| 9 | 37 |
| 10 | 39 |
| 11 | 37 |
| 12 | 30 |
| 13 | 28 |
| 14 | 34 |
| 15 | 37 |
| 16 | 29 |
| Result | 31 |

After Altered 10th position (3 -> 6) in original key

Ansary’s in hex: 416E736172792773

MDAnsary in hex: 4D44416E7**6**617279

After encryption we get:

setKey(4d44416e76617279)

encryptDES(416e736172792773)

IP: L0=bfb442ed, R0=00fe22d6

Rnd1 f(R0=00fe22d6, SK1=3c 09 19 2e 08 19 28 13 ) = 6b53ad9f

Rnd2 f(R1=d4e7ef72, SK2=3c 09 3b 32 2a 20 0c 18 ) = 01f200a8

Rnd3 f(R2=010c227e, SK3=3d 0f 09 32 24 15 0c 06 ) = 806e8b48

Rnd4 f(R3=5489643a, SK4=29 2d 1d 16 15 00 0a 20 ) = 17cbb9c4

Rnd5 f(R4=16c79bba, SK5=1b 25 0d 17 34 02 21 0d ) = c7d72c52

Rnd6 f(R5=935e4868, SK6=0b 3d 05 39 08 2b 0a 18 ) = 8bde44c2

Rnd7 f(R6=9d19df78, SK7=23 34 07 3b 0c 13 14 23 ) = 39a1ae1a

Rnd8 f(R7=aaffe672, SK8=2f 34 2e 19 0b 20 20 22 ) = 39994619

Rnd9 f(R8=a4809961, SK9=0f 35 26 0b 04 24 07 22 ) = 41531188

Rnd10 f(R9=ebacf7fa, SK10=0e 32 27 0d 31 08 24 01 ) = 7f1f8749

Rnd11 f(R10=db9f1e28, SK11=06 16 32 1d 30 22 19 18 ) = 9c7b7752

Rnd12 f(R11=77d780a8, SK12=15 12 36 3c 1e 19 0c 08 ) = d5699d3e

Rnd13 f(R12=0ef68316, SK13=35 2a 32 25 04 05 10 2a ) = 36b824bf

Rnd14 f(R13=416fa417, SK14=36 3a 38 26 13 03 20 24 ) = 3c1fdaea

Rnd15 f(R14=32e959fc, SK15=3a 0b 1a 2e 28 06 23 38 ) = 2d10ede2

Rnd16 f(R15=6c7f49f5, SK16=38 1b 1a 26 30 36 30 01 ) = aefbc0d1

FP: L=2f30e3ed, R=76a3aa46

returns 2f30e3ed76a3aa46

Again for this converting each round into 16 bit hex value:

|  |  |
| --- | --- |
| Round | 16 bit Hex |
| 1 | 00fe22d6d4e7ef72 |
| 2 | d4e7ef72010c227e |
| 3 | 010c227e5489643a |
| 4 | 5489643a16c79bba |
| 5 | 16c79bba935e4868 |
| 6 | 935e48689d19df78 |
| 7 | 9d19df78aaffe672 |
| 8 | aaffe672a4809961 |
| 9 | a4809961ebacf7fa |
| 10 | ebacf7fadb9f1e28 |
| 11 | db9f1e2877d780a8 |
| 12 | 77d780a80ef68316 |
| 13 | 0ef68316416fa417 |
| 14 | 416fa41732e959fc |
| 15 | 32e959fc6c7f49f5 |
| 16 | 6c7f49f59c12992d |
| Result | 2f30e3ed76a3aa46 |

Now comparing the changes for each round:

|  |  |
| --- | --- |
| Round | Total Digit Changed |
| 1 | 2 |
| 2 | 9 |
| 3 | 25 |
| 4 | 36 |
| 5 | 38 |
| 6 | 37 |
| 7 | 31 |
| 8 | 28 |
| 9 | 31 |
| 10 | 36 |
| 11 | 34 |
| 12 | 32 |
| 13 | 33 |
| 14 | 30 |
| 15 | 33 |
| 16 | 34 |
| Result | 34 |