



**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: Fall 2023

Assignment Topic: **DES Calculator**

Submitted on: **22/06/24**

Submitted by

Name: **Nafisa Tasnim Neha**

Student ID: **20200204020**

Lab Section: **A2**

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

**Given Data:**

- The Original text "CyberLab"
- The Original key "Security"
- Trace level: 2: +rounds

**Let's convert our experimental data into hexadecimal values for use in the DES calculator:**

The original text "CyberLab" converts to hexadecimal as 43796265724c6162. Similarly, the original key "Security" converts to hexadecimal as 5365637572697479.

**Here are the findings from our observation using DES encryption:**

- Input: The original text "43796265724c6162" and key "5365637572697479".
- Settings: Trace level set to 2, with detailed round information (+rounds).
- Result: The encrypted value obtained is "5bcea65ef04c0ba0".

## DES Calculator

DES Block Cipher Calculator

**Input Data (in hex)** 43796265724c6162

**DES Key (in hex)** 5365637572697479

**Encrypted value is:** 5bcea65ef04c0ba0

**Trace of DES Calculations or Errors**

**Trace Level:** ☐ 0: none ☐ 1: calls ☒ 2: +rounds

```
setKey(5365637572697479)
encryptDES(43796265724c6162)
IP: L0=ff12284b, R0=00de2295
Rnd1 f(R0=00de2295, SK1=3c 0b 19 2e 1d 12 20 30 ) = 72784489
Rnd2 f(R1=8d6a6cc2, SK2=3c 0b 3b 36 20 2c 0a 05 ) = 0c5938b7
Rnd3 f(R2=0c871a22, SK3=3d 0f 19 32 34 20 1e 01 ) = 0d28ecf7
Rnd4 f(R3=80428035, SK4=39 2d 1d 36 26 20 0c 09 ) = 3c87ba10
Rnd5 f(R4=3000a032, SK5=3b 2d 0d 17 14 27 0c 00 ) = 900992ac
Rnd6 f(R5=104b1299, SK6=0b 3d 0d 3b 1c 02 04 28 ) = d51cd1c9
Rnd7 f(R6=e51c71fb, SK7=2b 35 07 3b 38 03 20 0a ) = 309f6662
Rnd8 f(R7=20d474fb, SK8=2f 34 2f 19 19 03 08 3a ) = d9134bd5
Rnd9 f(R8=3c0f3a2e, SK9=0f 35 27 1b 22 2c 14 01 ) = 9c780fc9
Rnd10 f(R9=bcac7b32, SK10=0f 36 27 0d 12 24 1c 04 ) = 575aa01a
Rnd11 f(R10=6b559a34, SK11=06 36 36 1d 36 04 06 08 ) = 00723aec
Rnd12 f(R11=bcde41de, SK12=17 12 36 3d 30 05 08 09 ) = dabef3d8
Rnd13 f(R12=b1eb69ec, SK13=35 3a 32 2d 34 23 08 28 ) = e8e2b9bc
Rnd14 f(R13=543cf862, SK14=36 3a 3a 26 2c 01 2c 28 ) = fb26e0f6
Rnd15 f(R14=4acd891a, SK15=3e 0b 3a 2e 04 03 28 32 ) = c2a8932d
Rnd16 f(R15=96946b4f, SK16=38 1b 3a 26 22 04 07 05 ) = 71d4a75b
FP: L=5bcea65e, R=f04c0ba0
returns 5bcea65ef04c0ba0
```

### Initially, with:

- Original text: "43796265724c6162"
- Original key: "5365637572697479"
- Trace level: 2, with detailed round tracking (+rounds)
- We obtain an encrypted value of "5bcea65ef04c0ba0".

### After altering just one bit in the original text:

- New original text: "53796265724c6162"
- The resulting encrypted value shifts significantly to "b2bd3c99c6a75006".

## DES Calculator

DES Block Cipher Calculator

**DES Block Cipher Calculator**

Input Data (in hex) 53796265724c6162

DES Key (in hex) 5365637572697479

Encrypted value is: b2bd3c99c6a75006

Encrypt Decrypt About Quit

**Trace of DES Calculations or Errors**

Trace Level: ☐ 0: none ☐ 1: calls ☒ 2: +rounds

```
setKey(5365637572697479)
encryptDES(53796265724c6162)
IP: L0=ff13284b, R0=00de2295
Rnd1 f(R0=00de2295, SK1=3c 0b 19 2e 1d 12 20 30 ) = 72784489
Rnd2 f(R1=8d6b6cc2, SK2=3c 0b 3b 36 20 2c 0a 05 ) = 2d5d2877
Rnd3 f(R2=2d830ae2, SK3=3d 0f 19 32 34 20 1e 01 ) = eb452ea7
Rnd4 f(R3=662e4265, SK4=39 2d 1d 36 26 20 0c 09 ) = 9dfae97c
Rnd5 f(R4=b079e39e, SK5=3b 2d 0d 17 14 27 0c 00 ) = 911a20e3
Rnd6 f(R5=f7346286, SK6=0b 3d 0d 3b 1c 02 04 28 ) = 8fe29121
Rnd7 f(R6=3f9b72bf, SK7=2b 35 07 3b 38 03 20 0a ) = 6b9e668f
Rnd8 f(R7=9caa0409, SK8=2f 34 2f 19 19 03 08 3a ) = 301801ac
Rnd9 f(R8=0f837313, SK9=0f 35 27 1b 22 2c 14 01 ) = 21e31bf7
Rnd10 f(R9=bd491ffe, SK10=0f 36 27 0d 12 24 1c 04 ) = d627ecc3
Rnd11 f(R10=d9a49fd0, SK11=06 36 36 1d 36 04 06 08 ) = 03040273
Rnd12 f(R11=be4d1d8d, SK12=17 12 36 3d 30 05 08 09 ) = 0871dd09
Rnd13 f(R12=d1d542d9, SK13=35 3a 32 2d 34 23 08 28 ) = cb0734be
Rnd14 f(R13=754a2933, SK14=36 3a 3a 26 2c 01 2c 28 ) = a008e902
Rnd15 f(R14=71ddabdb, SK15=3e 0b 3a 2e 04 03 28 32 ) = 4e6d2782
Rnd16 f(R15=3b270eb1, SK16=38 1b 3a 26 22 04 07 05 ) = 21921df1
FP: L=b2bd3c99, R=c6a75006
returns b2bd3c99c6a75006
```

No.		Binary	Difference
	43796265724c6162 53796265724c6162	0100001101111001011000100110010101110010010011000110000101100010 0101001101111001011000100110010101110010010011000110000101100010	1
1	00de22958c6e6c42 00de22958c6f6c42	0000000011011110001000101001010110001100011011100110110001000010 0000000011011110001000101001010110001100011011110110110001000010	1
IP <sup>-1</sup>	d416d19674f02038 bf72f9df32a8ae05	1101010000010110110100011001011001110100111100000010000000111000 101111110111001011111001110111100110010101010001010111000000101	28

If a single value is altered in the original text, the encryption process results in a total of **28 bits** being changed after the inverse permutation stage.

#### Initially encrypted with:

- Original text: "43796265724c6162"
- Original key: "5365637572697479"
- Trace level: 2, with detailed round tracking (+rounds)
- The ciphertext is generated as "5bcea65ef04c0ba0".

After changing just one bit in the original key to "536563757269747**6**", the encrypted value substantially transforms to "**d0f5f1b470454771**".

## DES Calculator

DES Block Cipher Calculator
— □ ×

### DES Block Cipher Calculator

**Input Data (in hex)**

**DES Key (in hex)**

**Encrypted value is:**

43796265724c6162

5365637572697476

d0f5f1b470454771

Encrypt
Decrypt
About
Quit

**Trace of DES Calculations or Errors**

**Trace Level:**    ☐ 0: none    ☐ 1: calls    ☒ 2: +rounds

```

setKey(5365637572697476)
encryptDES(43796265724c6162)
IP:      L0=ff12284b, R0=00de2295
Rnd1    f(R0=00de2295, SK1=3c 0b 19 2e 1d 12 04 34 ) = 727a4ca8
Rnd2    f(R1=8d6864e3, SK2=3c 0b 3b 36 21 2c 0a 05 ) = 06bb8496
Rnd3    f(R2=0665a603, SK3=3d 0f 19 32 14 22 1f 01 ) = 0c3d7652
Rnd4    f(R3=815512b1, SK4=39 2d 1d 36 2e 28 04 09 ) = 7d90b2a5
Rnd5    f(R4=7bf514a6, SK5=3b 2d 0d 17 10 27 1c 02 ) = 37d10d07
Rnd6    f(R5=b6841fb6, SK6=0b 3d 0d 3b 1f 02 04 28 ) = 1f1d5fa7
Rnd7    f(R6=64e84b01, SK7=2b 35 07 3b 38 05 21 0a ) = c217a0a1
Rnd8    f(R7=7493bf17, SK8=2f 34 2f 19 11 0b 08 3a ) = 630a7c84
Rnd9    f(R8=07e23785, SK9=0f 35 27 1b 22 0c 14 19 ) = e620ef67
Rnd10   f(R9=92b35070, SK10=0f 36 27 0d 12 35 18 04 ) = 9a1726aa
Rnd11   f(R10=9df5112f, SK11=06 36 36 1d 36 04 06 28 ) = a24926cf
Rnd12   f(R11=30fa76bf, SK12=17 12 36 3d 20 05 28 0d ) = 49719037
Rnd13   f(R12=d484b118, SK13=35 3a 32 2d 34 23 0a 30 ) = a2018a4e
Rnd14   f(R13=92fbfcf1, SK14=36 3a 3a 26 2c 10 2c 29 ) = 1e93fd33
Rnd15   f(R14=ca177c2b, SK15=3e 0b 3a 2e 04 23 28 12 ) = 9d65fcb1
Rnd16   f(R15=0f9e0040, SK16=38 1b 3a 26 26 00 07 07 ) = 3d8816cd
FP:      L=d0f5f1b4, R=70454771
returns d0f5f1b470454771
        
```

No.		Binary	Difference
	43796265724c6162 43796265724c6162	0100001101111001011000100110010101110010010011000110000101100010 0101001101111001011000100110010101110010010011000110000101100010	1
1	00de22958c6e6c42 00de22958d6864e3	0000000011011110001000101001010110001100011011100110110001000010 0000000011011110001000101001010110001100011011110110110001000010	1
IP <sup>-1</sup>	d416d19674f02038 0f9e0040f79f6ae6	1101010000010110110100011001011001110100111100000010000000111000 1011111011100101111001110111100110010101010001010111000000101	35

Altering a single value in the original key will cause **35 bits** to change in the

encryption process after the inverse permutation stage.

So, DES exhibits a strong avalanche effect. Small changes in the plaintext or key result in significant and unpredictable changes in the ciphertext. This characteristic is crucial for maintaining the security and unpredictability of the encryption process. The results demonstrate that DES achieves this effectively, as we observed numerous bit changes in the ciphertext after making minor alterations to the input.