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

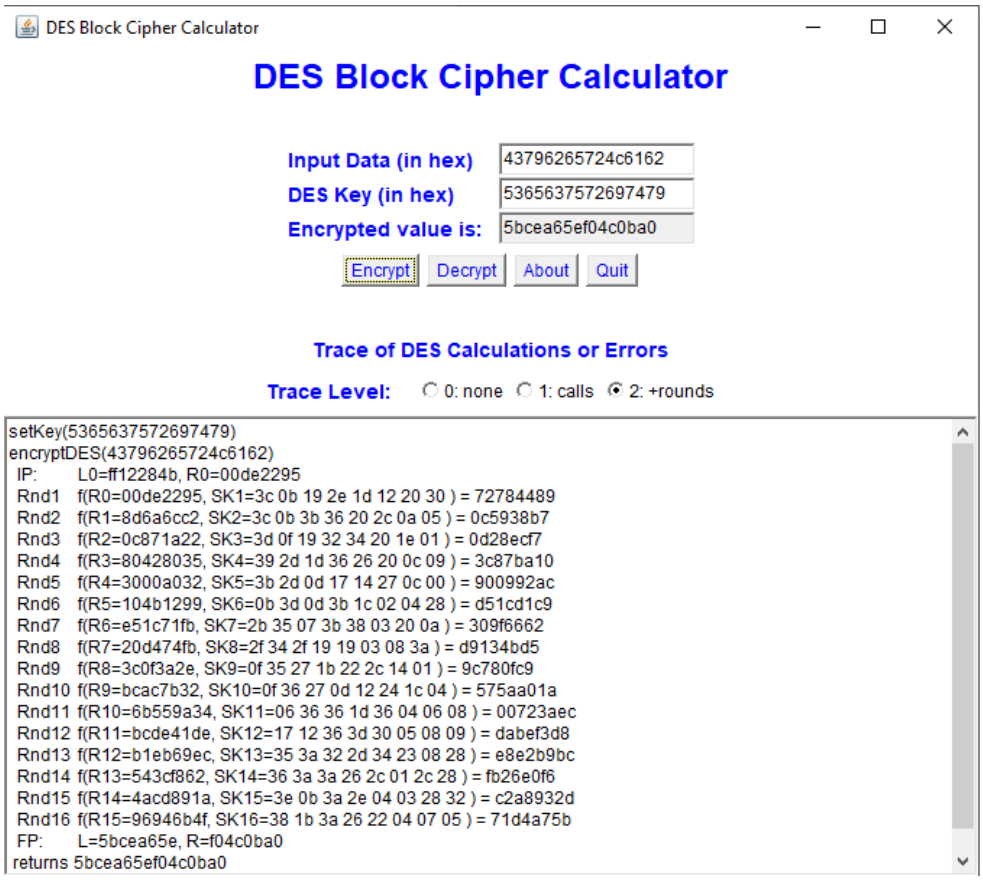
Let's convert our experimental data into hexadecimal values for use in the DES calculator:

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



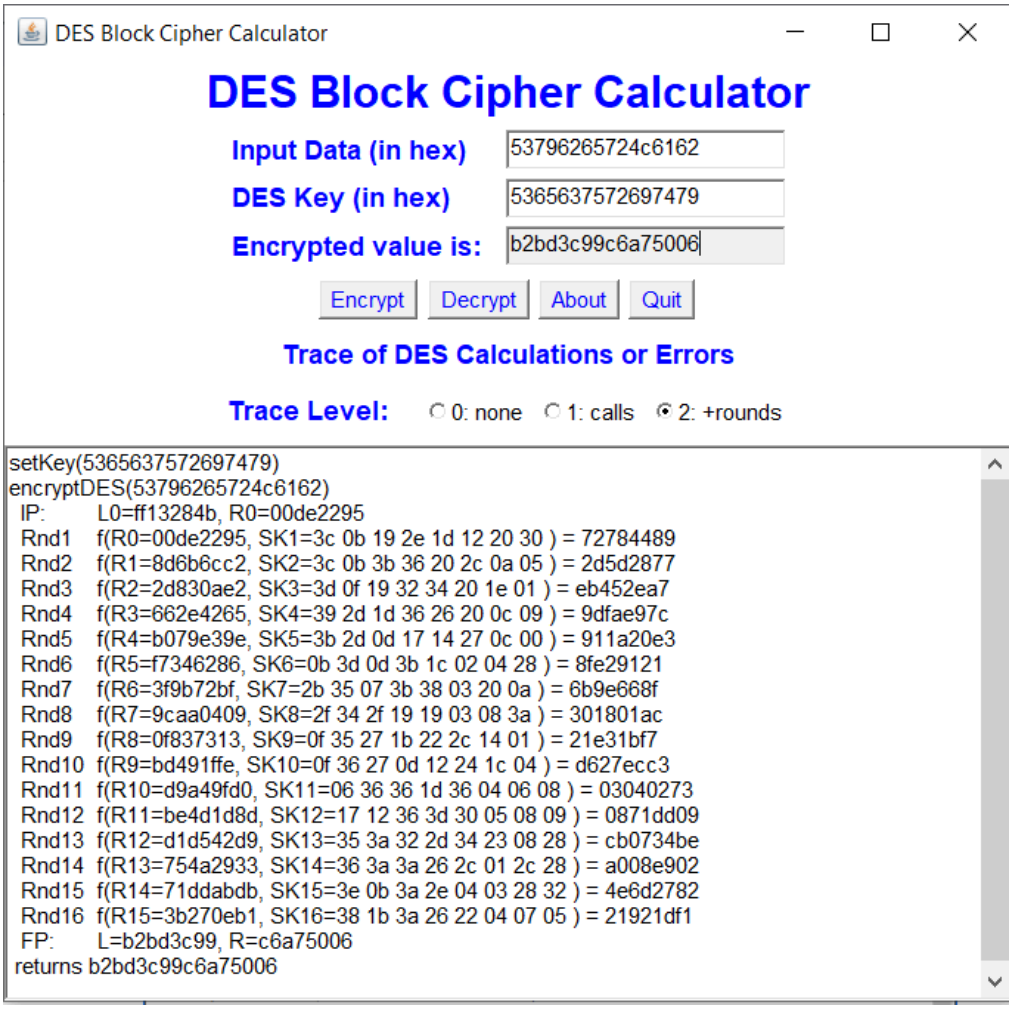
Initially, with:

- 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



No.		Binary	Difference
	43796265724c6162 53796265724c6162	0100001101111001011000100110010101110010010011000110000101100010 0101001101111001011000100110010101110010010011000110000101100010	1
1	00de22958c6e6c42 00de22958c6f6c42	0000000011011110001000101001010110001100011011100110110001000010 0000000011011110001000101001010110001100011011110110110001000010	1
IP^{-1}	d416d19674f02038 bf72f9df32a8ae05	1101010000010110110100011001011001110100111100000010000000111000 1011111101110010111110011101111100110010101010001010111000000101	28

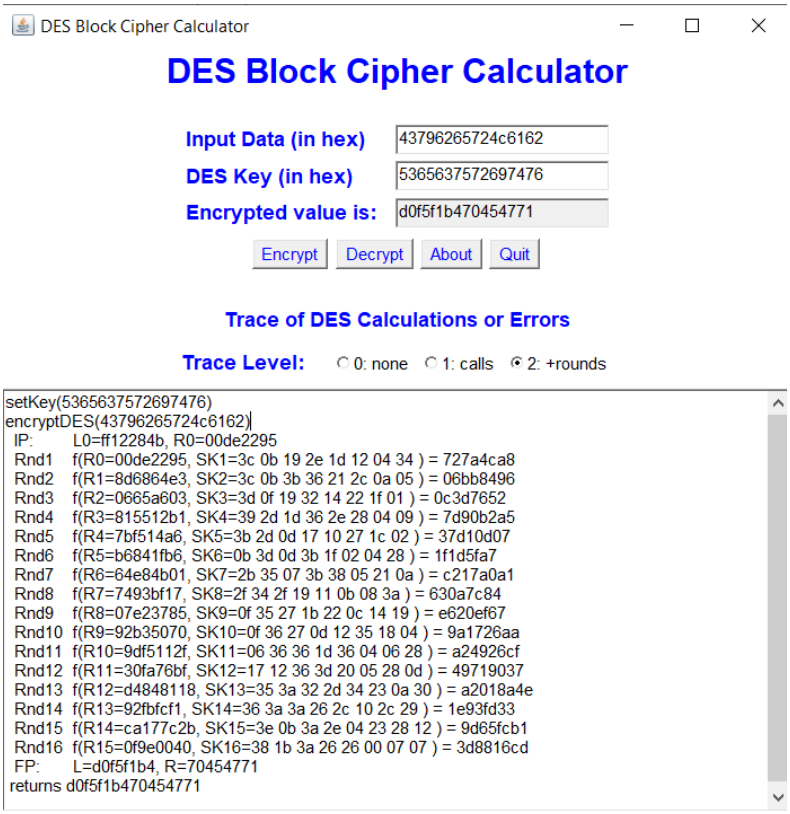
If a single value is altered in the original text, the encryption process results in a total of **28 bits** being changed after the inverse permutation stage.

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 "5365637572697476", the encrypted value substantially transforms to "**d0f5f1b470454771**".

DES Calculator



No.		Binary	Difference
	43796265724c6162 43796265724c6162	0100001101111001011000100110010101110010010011000110000101100010 0101001101111001011000100110010101110010010011000110000101100010	1
1	00de22958c6e6c42 00de22958d6864e3	0000000011011110001000101001010110001100011011100110110001000010 0000000011011110001000101001010110001100011011110110110001000010	1
IP^{-1}	d416d19674f02038 0f9e0040f79f6ae6	1101010000010110110100011001011001110100111100000010000000111000 1011111101110010111110011101111100110010101010001010111000000101	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.