Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

REPORT

Laboratory Work Nr.4
Discipline: Cryptographic methods of information protection

Realised by: st.gr. FAF-213
Iațco Sorin

Checked by : asist.univ.
Mîțu Cătălin

Chișinău 2023

Subject: Block ciphers. The DES algorithm.

Tasks:

To develop a program in one of the programming languages preferred for implementing an element of the DES algorithm. The task will be chosen according to the order number n of the student from the group list, according to the formula: nr_task = n mod 11. For each task let the tables used and all intermediate steps be displayed on the screen. Input data be user-input or randomly generated.

Task 10. In round i of the DES algorithm, we know:
S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)

Calculate Ri, if it is known that Li-1= ... (32 bits).

DES Algorithm:

The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm used for data encryption. Here are the steps of the DES algorithm:

1. Initial Permutation (IP):
    - The 64-bit plaintext is permuted according to a fixed table to create the Initial Permutation.
2. Key Generation:
    - The 64-bit encryption key is used to generate 16 subkeys, one for each of the 16 rounds. Each subkey is 48 bits long.
3. Round Function:
    - DES consists of 16 rounds. In each round, the right half of the data (32 bits) is expanded to 48 bits using an expansion permutation.
    - The 48-bit result is then XORed with the current round's subkey.
4. Substitution (S-boxes):
    - The 48-bit result from the XOR operation is divided into 8 groups of 6 bits each.
    - Each 6-bit group is substituted using a set of 8 S-boxes, each with a predefined 4-bit output.
    - The output from the S-boxes is combined to produce a 32-bit result.
5. Permutation (P):
    - The 32-bit result from the S-boxes is permuted using a fixed table.

6. Feistel Network:
    - The Feistel network is used in DES. The right half of the data is XORed with the output of the permutation step and swapped with the left half.
7. Repeat Rounds:
    - Steps 3 through 6 are repeated for a total of 16 rounds.
8. Final Permutation (IP^-1):
    - After the 16 rounds, the left and right halves are swapped one last time.
    - The resulting 64-bit data is subjected to a final permutation, which is the inverse of the initial permutation.
9. Output:
    - The final 64-bit data is the ciphertext.

To decrypt a DES-encrypted message, the same steps are applied in reverse order using the same subkeys.

Results:

The S Boxes are predefined, as well as the Expansion table and the Permutation Table. Now the L_{i-1} and the subkey for this round i are generated randomly.

```
LiMinus1:  [0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1]
Subkey:  [1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0]
```

Figure 1. *Randomly generated input*

The tables used for this implementation are shown in the terminal.

```
Expansion Table:
32  1  2  3  4  5  4  5
 6  7  8  9  8  9 10 11
12 13 12 13 14 15 16 17
16 17 18 19 20 21 20 21
22 23 24 25 24 25 26 27
28 29 28 29 30 31 32  1

Permutation Table:
16  7 20 21 29 12 28 17
 1 15 23 26  5 18 31 10
 2  8 24 14 32 27  3  9
19 13 30  6 22 11  4 25
```

Figure 2. *Tables used*

Then, finnaly, after the round i was processed the result R_i is displayed.

```
Ri:
[1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0]
```

Figure 3. *Result* R_i

Conclusion:

In conclusion this laboratory work, I implemented a fundamental part of the Data Encryption Standard (DES) algorithm. DES is a classic symmetric-key block cipher encryption algorithm that was widely used for secure data communication in the past. The implemented part of the DES algorithm involves a single round of the Feistel network, which is the core structure of DES. The code provided allows to perform a single round of DES encryption, which can be part of a larger DES encryption or decryption process. In a complete DES implementation, these steps would be repeated for a total of 16 rounds.

Resources:

CS-Labs/lab4 at main · Syn4z/CS-Labs (github.com)