Ministry of Education, Culture and Research of the Republic of Moldova
Technical University of Moldova
Department of Software and Automation Engineering

REPORT

Laboratory work no. 4
Block ciphers. DES algorithm

Elaborated:
st. gr. FAF-213 Botnari Ciprian

Verified:
asist. univ. Cătălin Mîțu

Chişinău – 2023

Table of Contents

Topic: Block ciphers

Tasks

For DES algorithm in i round, K_i and R_{i-1} are known. Find out

$$B_1B_2B_3B_4B_5B_6B_7B_8$$

Theoretical notes

The Data Encryption Standard (DES) is a widely used symmetric-key block cipher designed to operate on 64-bit blocks of data. The DES algorithm consists of several key phases:

1. **Key Generation**: The process begins with a 64-bit encryption key, which is then subjected to a series of permutation and compression operations to generate 16 subkeys, each 48 bits in length, to be used in the 16 rounds of the DES algorithm.
2. **Initial Permutation (IP)**: The initial 64-bit plaintext block is rearranged through a specific permutation operation.
3. **16 Rounds (Feistel Network)**: Each round of DES consists of the following steps:
4. **Expansion (E)**: The right half of the 32-bit data is expanded to 48 bits by replicating certain bits.
5. **Subkey XOR (XOR with Round Key)**: XOR the 48-bit result from the expansion with the 48-bit subkey for the current round.
6. **S-Box Substitution**: Divide the 48-bit block into eight 6-bit blocks. Substitute each 6-bit block using one of eight S-boxes, resulting in eight 4-bit blocks. S-boxes perform complex bit-shuffling and substitution, increasing confusion.
7. **Permutation (P)**: After substitution, concatenate the eight 4-bit blocks into a 32-bit block. Apply a fixed permutation (P-box) to rearrange the bits.
8. **Swap Left and Right Halves**: Swap the left and right 32-bit halves of the data and proceed to the next round.
9. **Inverse Initial Permutation (IP^-1)**: After 16 rounds, combine the left and right halves. Apply the inverse of the initial permutation to generate the 64-bit ciphertext block.
10. **Decryption**: Decryption in DES mirrors encryption, but the subkeys are used in reverse order (last subkey first). The same operations (expansion, S-boxes, permutation, etc.) are applied in reverse to obtain the original plaintext.
11. **Key Schedule and Subkey Generation**: The key schedule generates the 16 round subkeys. Each subkey is generated from the original 64-bit key through a series of permutations and shifts.

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

Table 1. Expansion

Results

Let's choose the key k = 1101011010011101010101011101110101011101010101 and r = 00110011001100110011001100110011. The results are as follows:

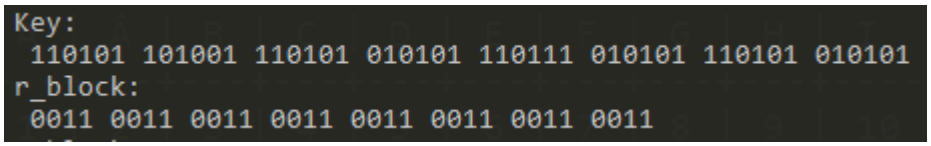

Figure 1. *Manual input*

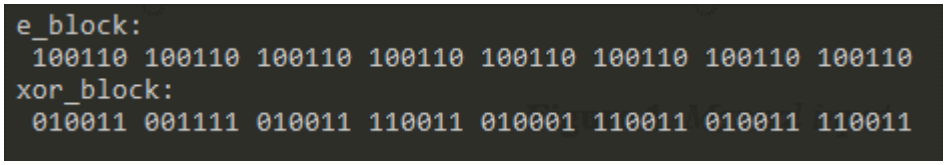

Figure 2. *Manual output*

The results for random input:

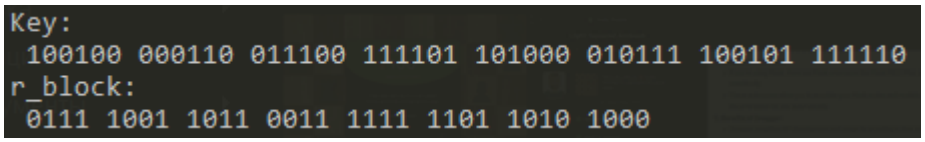

Figure 3. *Random input*

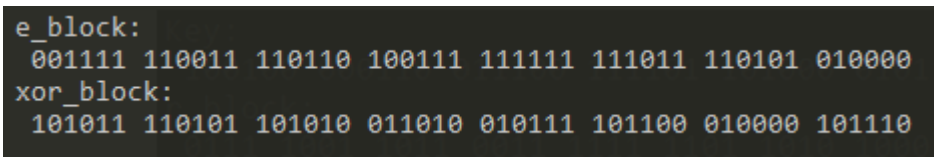

Figure 4. *Random output*

Conclusion

In conclusion, the exploration of the Data Encryption Standard (DES) has offered valuable insights into the realm of cryptographic techniques. This laboratory work has equipped me with practical experience in both the encryption and decryption processes using DES, a pivotal cryptographic algorithm in the history of information security. Furthermore, it has become evident that DES provided a significant leap in the level of security compared to its predecessors, showcasing its importance in safeguarding sensitive information.

Github

Sufferal/cryptography-labs (github.com)