Lucrare de laborator nr. 4

Cifruri bloc. Algoritmul DES

Sarcina 1. Studiați materiale didactice plasate pe ELSE:

- *C4. Cifruri bloc*
- *DES-FIPS-46*
- *DES-FIPS-46-3*
- *Theory of Data Encryption Standard (DES)*
- *ASCII Character Set*
- *DES eng*
- *DES RO*

***Sarcina* 2**. **De elaborat un program în unul din limbajele de programare preferate pentru implementarea unui element al algoritmului DES. Sarcina se va alege în conformitate cu numărul *n* de ordine al studentului din lista grupei, în conformitate cu formula: nr_sarcina = *n* mod 11. Pentru fiecare sarcină să fie afișate la ecran tabelele utilizate și toți pașii intermediari. Datele de intrare să fie posibil de introdus de utilizator sau de generat în mod aleatoriu.**
Atenție! La susținerea lucrării vor fi puse întrebări despre lucrul întregului algoritm!!!

Lista de sarcini

2.1. Fiind dată cheia algoritmului DES (8 simboluri), de determinat $K+$.
2.2. Fiind dat $K+$ în algoritmului DES, de determinat C_i și D_i pentru un i dat.
2.3. În algoritmul *DES* este dat $K+$. Să se determine cheia de rundă K_i pentru un i dat.
2.4. În algoritmul *DES* este dat mesajul (8 caractere). De aflat L_1.
2.5. În algoritmul *DES* este dat $K+$. Să se determine toate cele 16 chei de rundă K_i.
2.6. În algoritmul *DES* în runda i este cunoscut K_i și R_{i-1}. De calculat
$$B_1B_2B_3B_4B_5B_6B_7B_8$$
2.7. În algoritmul *DES* este dat $B_1B_2B_3B_4B_5B_6B_7B_8$
De aflat
$$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$
2.8. Să se calculeze R_i pentru runda k a algoritmului DES, dacă se cunoaște L_{k-1} și rezultatul aplicării cutiilor-*S*.
2.9. În runda i a algoritmului DES am obținut $K_i + E(R_{i-1}) = ...$ (48 biți)
Să se determine $S_j(B_j)$ pentru un j dat.

2.10. În runda *i* a algoritmului DES se cunoaște:

$$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$

Să se calculeze R_i, dacă se cunoaște că L_{i-1}= ... (32 biți).

2.11. La criptarea unui bloc în cifrul DES s-a obţinut

L_{16} = ... (32 biți)

R_{16} = ... (32 biți)

Să se determine blocul criptat al mesajului reprezentat hexazecimal.

***Notă*: Cine nu realizează o aplicație - poate opta pentru următoarea sarcină alternativă (nota maximă fiind 9):**

- **de realizat criptarea blocului *i* a mesajului *m*, utilizând algoritmul DES cu cheia *k*, considerând o versiune scurtată, formată dintr-o singură rundă (permutarea finală va fi realizată la sfârșitul rundei 1);**
- **mesajul criptat va fi reprezentat hexazecimal;**
- **indicele *i* al blocului de biți și cheia *k* se vor solicita de la profesor.**

m *= The Data Encryption Standard (DES) specifies two FIPS approved cryptographic algorithms as required by FIPS 140-1. When used in conjunction with American National Standards Institute (ANSI) X9.52 standard, this publication provides a complete description of the mathematical algorithms for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithms described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.*