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

**Discipline**: Cryptography and Security

Elaborated: Vlad Protean FAF-222,

Checked: asist. univ. Dumitru Nirca,

Chișinău 2023

Topic: **Cifruri bloc. Algoritmul DES**

Tasks:

**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!!!**

Theoretical notes:

Metoda de criptare cunoscută sub numele de „cifrul Vigenère” a fost atribuită greșit lui

Blaise de Vigenère în secolul al XIX-lea și, de fapt, a fost descrisă pentru prima dată de Giovan

Battista Bellaso în cartea sa din 1553 La cifra del. Sig. Vigenère a creat un cifru asemănător, dar

totuși diferit și mai puternic în 1586.

Pe da altă parte, cifrul Vigenere folosește aceleași operații ca și cifrul Cezar. Cifrul

Vigenere și fel deplasează literele, dar, spre deosebire de Cezar, nu se poate sparge ușor în 26

combinații. Cifrul Vigenere folosește o deplasare multiplă. Cheia nu este constituită de o singură

deplasare, ci de mai multe, fiind generate de câțiva întregi ki, unde 0 ≤ ki ≤ 25, dacă luăm ca reper

alfabetul latin cu 26 de litere. Criptarea se face în felul următor:

ci = (mi + ki) mod 26.

Cheia poate fi, de exemplu, k = (5, 20, 17, 10, 20, 13) și ar provoca deplasarea primei litere

cu 5, c1=m1 + 5 (mod 26), a celei de a doua cu 20, c2 = m2 + 20 (mod 26), ș.a.m.d. până la sfârșitul

cheii și apoi de la început, din nou. Cheia este de obicei un cuvânt, pentru a fi mai ușor de memorat

– cheia de mai sus corespunde cuvântului „furtun”. Metoda cu deplasare multiplă oferă protecție

suplimentară din două motive:

• primul motiv este că ceilalți nu cunosc lungimea cheii;

• cel de al doilea motiv este că numărul de soluții posibile crește odată cu mărimea cheii;

de exemplu, pentru lungimea cheii egală cu 5, numărul de combinații care ar fi

necesare la căutarea exhaustivă ar fi 265 = 11 881 376.

Decriptarea pentru cifrul Vigenere este asemănătoare criptării. Diferența constă în faptul

că se scade cheia din textul cifrat,

mi = (ci – ki) mod 26.

Pentru simplificarea procesului de cifrare se poate utiliza următorul tabel, numit Tabula

Recta (tabelul 3.1), care se utiliza de către Vigenere. Aici toate cele 26 cifruri sunt situate pe

orizontală și fiecărui cifru îi corespunde o anumită literă din cheie, reprezentată în colana din

stânga tabelului. Alfabetul corespunzător literelor textului clar se află în prima linie de sus a

tabelului. Procesul de cifrare este simplu – este necesar ca având litera mi din mesaj și litera ki din1cheie să găsim litera textului cifrat ci, care se află la intersecția liniei mi și coloanei ki. În exemplul

din tabelul 3.1 este prezentat cazul mi = M și ki = H, iar în rezultat se obține ci = T.

**Implementation()**

**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.**