**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**



*Laboratory work 3*

Subject: Criptanaliza Cifrul Vigenère

Done by: Sirețanu Andreia-Cristina

st. gr. FAF-211

Verified by: Mitu Cătălin

Chişinău - 2023

**Subiectul:** Cifrul Vigenère

**Sarcini:**

De implementat algoritmul Vigenere în unul din limbajele de programare pentru mesaje în limba română (31 de litere), acestea fiind codificate cu numerele 0, 1, ... 30. Valorile caracterelor textului sunt cuprinse între ‘A’ și ’Z’, ’a’ și ’z’ și nu sunt premise alte valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect al caracterelor. Lungimea cheii nu trebuie să fie mai mică de 7. Criptarea și decriptarea se va realiza în conformitate cu formulele din modelul matematic prezentat mai sus. În mesaj mai întâi trebuie eliminate spațiile, apoi toate literele se vor transforma în majuscule. Utilizatorul va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau criptograma și va obține criptograma sau mesajul decriptat.

**Etapele efectuării sarcinilor:**

1. Am electuat tabelul cu indexuri pentru alfabetul român:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | Ă | Â | B | C | D | E | F | G | H | I | Î | J | K | L | M | N | O | P | Q |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| R | S | Ș | T | Ț | U | V | W | X | Y | Z |  |  |  |  |  |  |  |  |  |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |  |  |  |  |  |  |  |  |  |

*Figura1. Literele alfabetului roman și indexul acestora*

2. Transformam cheia și textul dat in stringuri cu caractere majuscule și fără spații:

“Șoseaua este nou asfaltată” => ȘOSEAUAESTENOUASFALTATĂ

“O viață frumoasă” => OVIAȚĂFRUMOASĂ

3. Indicăm la fiecare caracter din aceste 2 stringuri numărul corespunzător conform alfabetului, completăm spațiile goale dintre stringuri cu characterele cheii repetate de la început.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ș | O | S | E | A | U | A | E | S | T | E | N | O | U | Ă |
| 22 | 17 | 21 | 6 | 0 | 25 | 0 | 6 | 21 | 23 | 6 | 16 | 17 | 25 | 1 |
| O | V | I | A | Ț | Ă | F | R | U | M | O | A | S | Ă | O |
| 17 | 26 | 10 | 0 | 24 | 1 | 7 | 20 | 25 | 15 | 17 | 0 | 21 | 1 | 17 |

*Figura2. Literele textului dat și a cheiei date și indexul acestora conform alfabetului*

4. Pentru codificare luăm fiecare coloană din tabelul de mai sus și introducem în formula:

(nr1 + nr2) % 31

nr1 – numărul din tabel a characterului textului.

nr2 – numărul din tabel a characterului cheiei.

31 – numărul total de litere în alfabetul roman.

5. Obținem următorul șir de numere pe care le convertim înapoi în litere conform primei figuri.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 12 | 0 | 6 | 24 | 26 | 7 | 26 | 15 | 7 | 23 | 16 | 7 | 26 | 17 |
| G | J | A | E | Ț | V | F | V | M | F | T | N | F | V | O |
| 16 | 17 | 0 | 7 | 24 | 7 | 12 | 26 |  |  |  |  |  |  |  |
| N | O | A | F | Ț | F | J | V |  |  |  |  |  |  |  |

*Figura3. Codul codificat*

4. Pentru dodificare efectuăm aceleași acțiuni folosind numai formula:

(nr1 - nr2) % 31

nr1 – numărul din tabel a characterului textului.

nr2 – numărul din tabel a characterului cheiei.

31 – numărul total de litere în alfabetul roman.

**Concluzie:** Folosind Cifrul Vigenère am învățat o metodă nouă, interesantă și utilă de criptare a informației ce ma ajutat la soluționarea descifrării și codării unui anumit text dintr-un anumit alfabet cu o anumită cheie. Ma învățat să gândesc într-un mod abstract și logic, având multă răbdare în activitatea aceasta.