Cifrul Nicodemus

Pentru a cripta un mesaj avem nevoie de text clar și cheie. Datorită faptului că cifrul Nicodemus este modular, putem folosi diverse metode de permutare și substituție. În cazul dat voi folosi substituția Vigenere și transpoziția pe coloană, ambele în bza cheii date. Inițial formăm un tabel bidimensional de lățime egală cu lungimea cheii, atribuind primului rând caracterele cheii, iar în continuare completând tabelul c ucaracterele textului clar. Mai departe, din cheie formăm șirul de numere, în baza căruia vom rearanja coloanele. Șirul dat se formează prin marcarea ordinii relative a caracterelor în baza alfabetului. În cazul dat caracterele duplicate obțin valori diferite.

```
TOMATO -> 532164
```

În continumare rearanjăm coloanele astfel, ca seria de ordonare să se transforme într-o serie consecutivă. Mai departe vom folosi algoritmul Vigenere, criptând toate șirurile în afară de primul, folosind primul șir ca și cheie (de fapt cheie ordonată alfabetic). În final, excludem primul rând din tabel și îl împărțim în blocuri de 5 rânduri (valoare standartă). În continuare luăm fiecare bloc și extragem fiecare coloană ca șir de caractere, care și formează textul criptat.

Pentru a decripta un mesaj ordinea este inversă algoritmului de mai sus. Singura problemă care poate apărea este ordonarea corectă a textului în tabel. Inițial împărțim textul în șiruri de lungime 5 * lungimea cheii. Șirurile complete se aranjează în blocuri de 5 rânduri (analog extragerii acestora la criptare), în ultimul bloc aranjăm șiruri de lungimea cheii ca de obicei, iar în caz că rămânem cu un șir incomplet - vertificăm dacă coloana dată după transpoziție ar avea vreun caracter (în dependență de numărul caracterelor rămase). Mai departe decriptăm folosind Vigenere și inversăm transpoziția pe coloane.