

# Cifrul Myszkowski

---

Pentru a cripta un mesaj avem nevoie de propriu-zis textul clar și cheie. În primul rând, folosim cheia pentru a forma șirul de numere, în baza căruia vom aranja coloanele. Șirul dat este format prin marcarea ordinii relative a numerelor date în baza alfabetului, astfel în șirul dat A este primul, M este al doilea, etc. Caracterele duplicate au aceeași valoare.

TOMATO -> 432143

Mai departe aranjăm textul clar într-un tabel astfel, ca să se formeze atâtea coloane câte caractere sunt în cheie. Careurile goale se completează cu caractere aleatoare. Fiecărei coloane îi corespunde câte un număr din șirul numeric al cheii. În sfârșit, pentru a obține textul criptat trebuie să luăm câte un caracter din tabel, din stânga la dreapta, de sus în jos, în ordinea numerelor obținute din cheie.

Pentru a decripta un mesaj, avem nevoie de text criptat și cheie. Obținem seria numerică în baza cheii și formăm tabloul bidimensional de lungime  $\text{encrypted/key} + 1$  și lățime ca și cheia. Aranjăm caracterele în tabel analog criptării, de la stânga la dreapta, de sus în jos și în ordinea seriei numerice. În final luăm fiecare rând din tabel și le concatenăm ca să obținem textul clar.