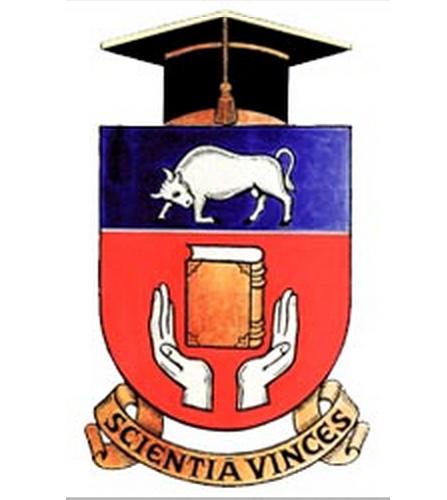
Universitatea de Stat din Tiraspol

Facultatea de Fizica Matematica si Informatica



Sistemul Afin

**Elaborat de**: Dordea Pavel, student gr.3i

**Verificat**: Globa Angela

**Chișinău, 2021**

***#Despre***

Cifrul afin este o generalizare a cifrului Cezar, având cheia k = {(a, b) | a, b ∈ Z26 = {0, 1, 2, …, 25}, cmmdc(a, 26) = 1}, iar funcţiile de criptare şi decriptare pentru o cheie k = (a, b) sunt ek(x) = ax + b (mod 26) și dk(y) = a −1(y+26 − b) (mod 26), unde a·a −1 =1 modn. Condiţia ca a să fie prim cu 26 asigură existenţa lui a −1 în Z26. Pentru calcularea lui a −1 poate fi aplicat algoritmul Euclid extins (vezi compartimentul 7), sau se verifică pa rând toate numerele reciproc prime cu a în clasa modulo n până când găsim acel număr pentru care a·a −1 =1 modn, acesta fiind și unicul cu o astfel de proprietate. De exemplu, pentru a = 7, b = 16 funcţia de criptare este ek(x) = 7x + 16. În acest caz pentru m =„cifrul afin”, obținem c =„ euzfap qzud”. Deoarece 7·15 =1 (mod26), avem 7−1 = 15 (mod 26), iar decriptarea se realizează matematic folosind funcţia 8 dk(y)= 15· (y+26−15)(mod 26)=15y+15·11 (mod 26)=15y + 9 (mod 26). Condiţia cmmdc(a, 26)=1 asigură de asemenea injectivitatea funcţiei ek, necesară pentru un proces corect de criptare-decriptare. De exemplu, pentru ek(x) = 10x + 1, A şi N se transformă ambele în B, iar O nu apare ca imagine în alfabetul substituţiei. În acest caz avem: cmmdc(a, 26)= cmmdc(10, 26)=2≠1. Astfel de cazuri au loc întotdeauna atunci când a nu respectă condiția de mai sus. Orice cheie k a cifrului afin este determinată complet de valorile întregi (a, b) pentru care cmmdc(a, 26) = 1. Sunt posibile 12 valori pentru a: 1, 3, 5, 7, 9, 11, 15, 19, 21, 23, 25 şi 26 valori pentru b, care se iau independent de a, cu o singură excepţie a = 1, b = 0 (care se exclude deoarece nu conduce la nici o criptare). Aşadar mulţimea cheilor în acest caz este alcătuită din 12·26–1=311 chei diferite, număr suficient de mic pentru atacul prin forţa brută, adică prin verificarea tuturor cheilor posibile. Trebuie de avut în vedere că în cazul în care este necesar de a cripta mesaje în limba română sau rusă (sau oricare altă limbă care are un alfabet) procedeul rămâne același, doar că trebuie să ținem cont de faptul că alfabetele respective au 31 și 33 de litere, adică n=31 și respectiv n=33.

***#Screenshots***



