



Cifrul Cezar

Implementare în VB.NET

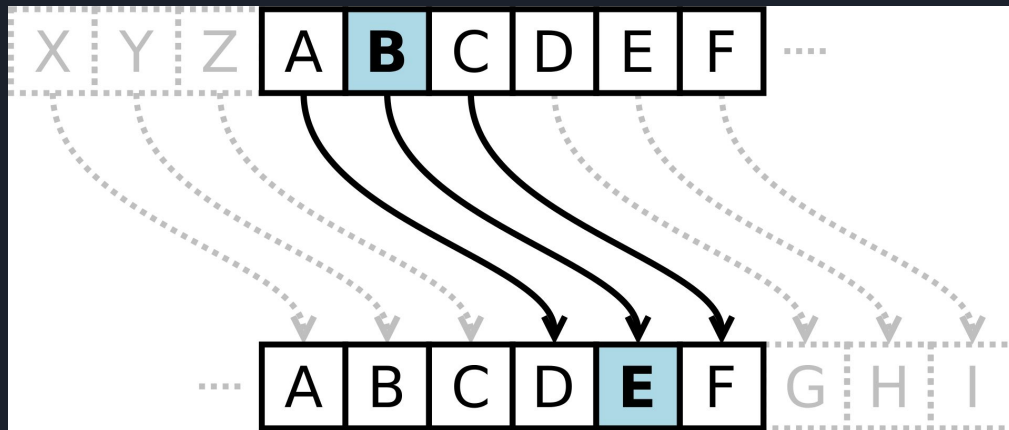
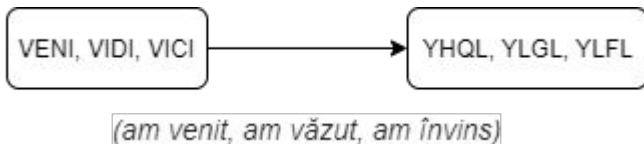


Cuprins

- ❖ *Scop*
- ❖ *Istorie*
- ❖ *Design*
- ❖ *Implementare*

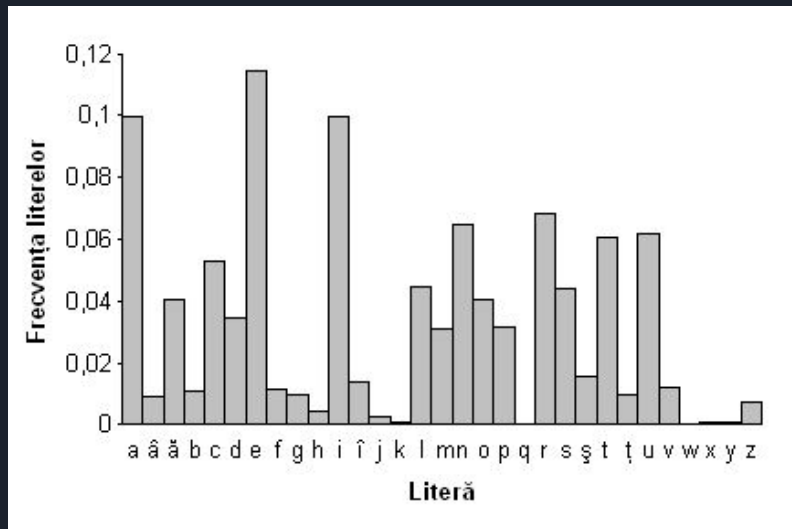
Scop

- ❖ Scopul Cifrului Cezar este de a transmite mesaje codificate, prin deplasarea cu un anumit număr a fiecărei litere și înlocuindu-se cu o alta litera dintr-un mesaj, astfel realizandu-se criptarea mesajului.
- ❖ Printr-un proces invers se poate realiza descifrarea unui mesaj deja codificat, astfel realizandu-se decriptarea mesajului.



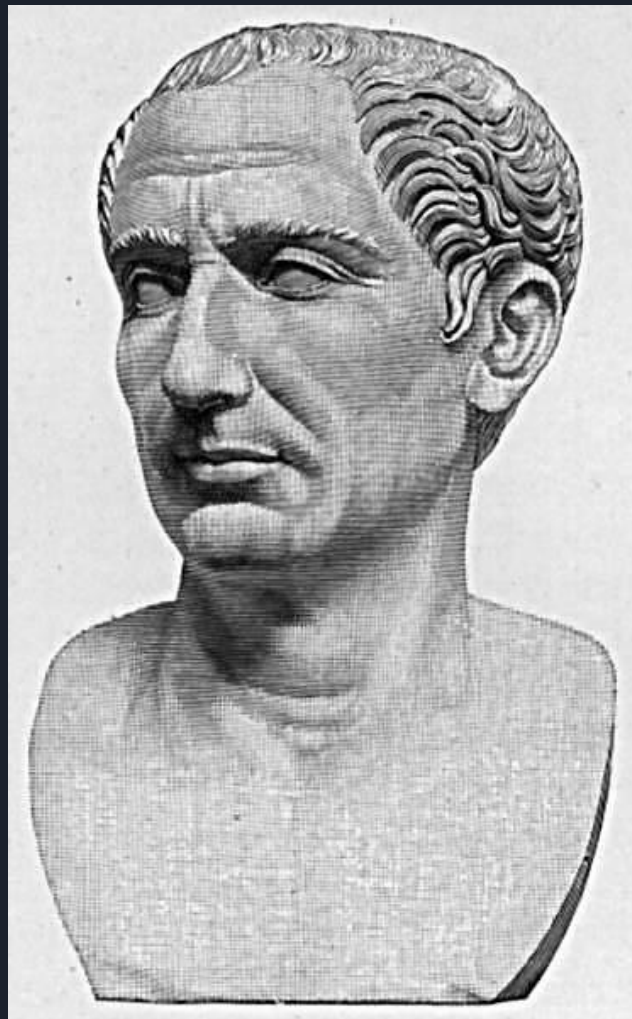
Cifrul Cezar

- ❖ În criptografie, cifrul lui Cezar, este una dintre cele mai cunoscute tehnici de criptare.



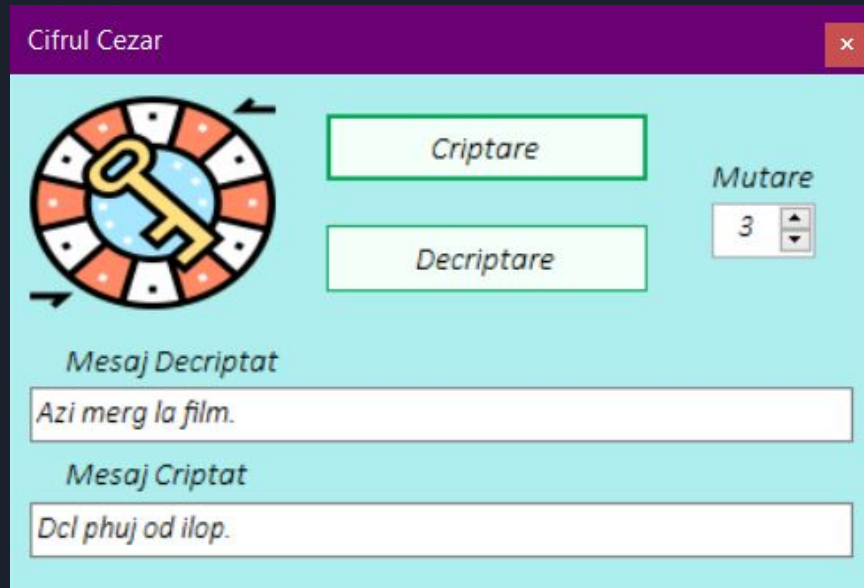
- ❖ Este un tip de cifru al substituției, în care fiecare literă din textul inițial este înlocuită cu o literă care se află în alfabet la o distanță fixă față de cea înlocuită. De exemplu, cu o deplasare de cinci poziții în alfabetul limbii române, A este înlocuit cu D, Ă devine E și așa mai departe. Această metodă este numită așa după Iulius Cezar, care o folosea pentru a comunica cu generalii săi.

- ❖ *Cifrul Cezar este denumit după Iulius Cezar, care îl folosea cu o deplasare de 3 pentru protejarea mesajelor cu importanță militară.*
- ❖ *Deși Cezar a fost primul care a fost folosit cifrul într-un mod în care se poate atesta, alte cifruri bazate pe substituție se cunosc ca fiind folosite anterior. Nepotul lui Iulius Cezar, Augustus, a folosit de asemenea cifrul, dar cu o deplasare de unu.*
- ❖ *Există dovezi cum că Iulius Cezar folosea și sisteme mai complicate, iar un scriitor, Aulus Gellius, referă un tratat (acum pierdut) despre cifrurile lui.*
- ❖ *Nu se știe cât de util era cifrul Cezar în acel timp, dar este probabil ca el să fie destul de sigur, atât timp cât numai câțiva dintre inamicii lui Cezar erau în stare să scrie și să citească, dar mai ales să cunoască concepte de criptanaliză.*



Design

- ❖ 1 x buton “Criptare”
 - apăsați pentru a se realiza criptarea
- ❖ 1 x buton “Decriptare”
 - apăsați pentru a se realiza decriptarea
- ❖ 1 x comboBox “Mutare”
 - setați numărul deplasării
- ❖ 1 x textBox “Mesaj Decriptat”
 - dați un mesaj
- ❖ 1 x textBox “Mesaj Criptat”
 - mesajul criptat generat/introdus





Implementarea Codului

- ❖ *Am creat o funcție de criptare:*
 - *aceasta funcție primește 3 parametrii.*
 - *dacă se efectuează criptarea atunci fiecărui caracter îi adunăm N mutări.*
 - *dacă se efectuează decriptarea atunci fiecărui caracter îi adunăm 26 și vom scădea N mutări.*
 - *pentru criptare/decriptare se va crea un nou șir care va fi returnat.*
- ❖ *Am creat un eveniment click pentru butonul “Criptare”:*
 - *acest buton apelează funcția de criptare și transmite șirul care se află în textBox-ul “Mesaj Decriptat”, numărul deplasării și un ‘true’ pentru ca funcția să efectueze criptarea.*
- ❖ *Am creat un eveniment click pentru butonul “Decriptare”:*
 - *acest buton apelează funcția de criptare și transmite șirul care se află în textBox-ul “Mesaj Criptat”, numărul deplasării și un ‘false’ pentru ca funcția să efectueze decriptarea.*

Mulumesc pentru
atenție !

