**MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA**

**UNIVERSITATE DE STAT “ALECU RUSSO” DIN BALȚI**

**FACULTATEA DE ȘTIINȚE REALE, ECONOMICE ȘI ALE MEDIULUI**

**CATEDRA DE MATEMATICA ȘI INFORMATICA**

**RAPORT**

**cu tema**

**„Dezvoltarea unei metode proprii de criptare.”**

**pentru unitatea de curs**

**„Securitatea sistemelor informatice”**

**A elaborat:**

**studentul gr. IS31R**

**Oselschi Pavel**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**A controlat:**

**asist. univ. Parahonco A.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Bălţi, 2025**

CUPRINS

[INTRODUCERE 3](#_Toc198499138)

[1. DESCRIEREA A ASPECTELOR TEORETICE ALE ALGORITMULUI PROPUS 4](#_Toc198499139)

[1.1. Criptarea 4](#_Toc198499140)

[1.2. Decriptarea 4](#_Toc198499141)

[2. DESCRIEREA A ASPECTELOR PRACTICE ALE ALGORITMULUI PROPUS 5](#_Toc198499142)

[CONCLUZII 6](#_Toc198499143)

# INTRODUCERE

În contextul actual al digitalizării accelerate, securitatea informațiilor reprezintă o prioritate fundamentală pentru sistemele informatice. Datele sensibile, precum informațiile personale, financiare sau confidențiale, sunt expuse constant riscurilor de interceptare, modificare sau acces neautorizat. Criptarea datelor joacă un rol esențial în protejarea confidențialității și integrității informațiilor, oferind o barieră împotriva atacurilor cibernetice. De-a lungul timpului, metodele de criptare au evoluat de la algoritmi simpli, precum cifrul lui Cezar, la soluții complexe, cum ar fi AES (Advanced Encryption Standard) sau RSA, care utilizează chei publice și private pentru a asigura securitatea comunicațiilor.

Acest raport își propune să dezvolte și să analizeze o metodă proprie de criptare, concepută pentru a ilustra principiile de bază ale securizării datelor într-un mod accesibil și practic. Algoritmul propus combină operațiuni precum deplasarea bitilor, multiplicarea modulară și operațiunea XOR, integrate cu o cheie secretă furnizată de utilizator. Scopul principal este de a transforma un mesaj clar într-o formă indescifrabilă fără cheia corespunzătoare, asigurând astfel confidențialitatea datelor. Spre deosebire de metodele standard, această abordare personalizată prioritizează simplitatea și claritatea, fiind destinată mai degrabă unui exercițiu educațional decât aplicațiilor critice de securitate.

Necesitatea dezvoltării unei metode proprii de criptare derivă din importanța înțelegerii mecanismelor fundamentale ale securității informatice. Prin explorarea procesului de criptare și decriptare, raportul evidențiază provocările legate de proiectarea unui algoritm eficient și rezistent la atacuri. De asemenea, se analizează limitele metodei propuse, oferind o bază pentru comparații cu soluțiile consacrate și pentru posibile îmbunătățiri viitoare. Astfel, această lucrare contribuie la aprofundarea cunoștințelor în domeniul securității sistemelor informatice, punând accent pe aplicabilitatea practică a conceptelor teoretice.

# DESCRIEREA A ASPECTELOR TEORETICE ALE ALGORITMULUI PROPUS

Algoritmul este simetric: aceeași cheie (între 1 și 20) este folosită pentru criptare și decriptare. Lucrează cu 62 de litere din alfabetul românesc (31 mici + 31 mari). Doar literele sunt criptate; restul caracterelor rămân la fel.

Pozițiile literelor sunt numărate ignorând caracterele speciale. La criptare: dacă poziția este pară, se adună cheia; dacă este impară, se scade. În decriptare se aplică invers. Astfel, rezultatul este reversibil. Se folosește operația „modulo” pentru a nu ieși din limitele alfabetului.

# 1.1. Criptarea

Criptarea presupune deplasarea fiecărei litere în alfabet. Dacă litera este pe o poziție pară, se adună cheia. Dacă este pe o poziție impară, se scade cheia. Literele mari rămân mari, iar cele mici rămân mici. Se folosește operația mod pentru a păstra indexul în limite.

Exemplu: cu cheia 3, litera „a” (poziția 0 – pară) devine „b”, iar „ș” (poziția 23 – impară) devine „q”. Astfel, „aș” devine „bq”.

# 1.2. Decriptarea

Decriptarea este procesul invers. La poziții pare, se scade cheia, iar la poziții impare, se adună. Dacă „bq” este textul criptat și cheia este 3: „b” → „a” și „q” → „ș”. Se obține textul original „aș”.

Această metodă este eficientă deoarece respectă structura limbii române și poate fi folosită fără internet, doar local, în aplicația web propusă.

# DESCRIEREA A ASPECTELOR PRACTICE ALE ALGORITMULUI PROPUS

Aplicația web este realizată cu HTML, CSS și JavaScript. Permite introducerea manuală a textului, încărcarea unui fișier text și alegerea unei chei între 1 și 20. Se pot cripta și decripta texte, iar rezultatul poate fi salvat ca fișier .txt.

Interfața este simplă, modernă și are mod întunecat (dark mode). JavaScript gestionează toate operațiile: validarea cheii, criptarea, decriptarea și exportul fișierului. Este complet funcțională offline și ideală pentru exerciții educaționale.

# CONCLUZII

Algoritmul propus este simplu, sigur pentru uz personal și didactic și poate fi ușor înțeles de oricine. Aplicația web permite experimentarea criptării într-un mod interactiv. Faptul că este adaptată alfabetului românesc o face unică și potrivită pentru mediul educațional din România.

Este utilă pentru testarea logicii criptării și pentru a învăța concepte fundamentale din criptografie într-un mod practic și accesibil.