**MINISTERUL EDUCAŢIEI AL REPUBLICII MOLDOVA**

**UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLŢI**

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

**CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ**

**Referat**

**La disciplina”Informatica generala”**

**ROLUL CRIPTOGRAFIEI IN SECURITATEA COMUNICATIILOR**

**Autor**

Studenta grupei IT11Z

**Vichilu Elena**

|  |
| --- |
|  |

**Conducător științific:**

Olesea SKUTNITKI

lect. Univ

|  |
| --- |
|  |

**BĂLȚI, 2022**

Cuprins

[Introducere 3](#_Toc102904811)

[Securitatea sistemelor informatice 4](#_Toc102904812)

[Atacuri asupra securitații sistemelor informatice 6](#_Toc102904813)

[Introducere în criptografie 7](#_Toc102904814)

[Criptografia clasică 8](#_Toc102904815)

[Securitatea criptării clasice 8](#_Toc102904816)

[Modelul criptării clasice 9](#_Toc102904817)

[Criptografia modernă 9](#_Toc102904818)

# Introducere

Informația a însemnat întotdeauna putere, prin urmare dorința de a o proteja, de a o face accesibilă doar unor elite, unor inițiați, s-a pus din cele mai vechi timpuri. Primele texte cifrate descoperite până în prezent datează de circa 4000 de ani și provin din Egiptul Antic.

Există date privind utilizarea scrierii cifrate în Grecia Antică încă din secolul al V-lea î.e.n. Pentru cifrare se folosea un baston în jurul căruia se înfășura, spirală lângă spirală, o panglică îngustă de piele, papirus sau pergament, pe care, paralel cu axa, se scriau literele mesajului. În Roma Antică, secretizarea informațiilor politice și militare se facea utilizând diverse tipuri de scrieri secrete; amintim cifrul lui Cesar, utilizat încă din timpul războiului galic. Contribuția arabă la dezvoltarea criptologiei, mai puțin cunoscută și mediatizată, este de o remarcabilă importanță. David Kahn, unul dintre cei mai de seamă istoriografi ai domeniului, subliniază în cartea sa The Codebreakers că, criptologia s-a născut în lumea arabă. Primele trei secole ale civilizației islamice (700-1000 e.n.) au constituit, pe lângă o mare extindere politică și militară și o epocă de intense traduceri în limba arabă ale principalelor opere ale antichității grecești, romane, indiene, armene, ebraice și siriene.

Unele cărți sursă erau scrise în limbi deja moarte, deci reprezentau în fapt texte cifrate, astfel încât traducerea lor constituie primii pași în criptanaliză, deci originile criptologiei pot fi atribuite arabilor. Dezvoltările criptanalizei au fost mult sprijinite de studiile lingvistice ale limbii arabe. Arabii au preluat cunoștințele matematice ale civilizațiilor grecești și indiene. Arabii sunt cei care au introdus sistemul zecimal de numerotație și cifrele “arabe”. Termenii “zero “, “algoritm”, “algebră” li se datoreză tot lor. Însuși termenul de “cifru” ne vine de la arabi. El provine de la cuvântul arab “sifr” care reprezintă traducerea în arabă a cifrei zero din 2009 - Anghel Cătălin Pagina 5 din 24 sanscrită. Conceptul de „zero” a fost deosebit de ambiguu la începuturile introducerii lui în Europa, în care sistemul de numerotație folosit era cel roman. De aceea se obișnuia să se spună despre cineva care vorbea neclar că vorbeste ambigu, ca un cifru. Acest înțeles de ambiguitate a unui mesaj poartă și azi denumirea de cifru. Prin urmare, putem concluziona că, încă din antichitate s-a încercat securizarea informației și a datelor transmise.

# Securitatea sistemelor informatice

Apariția și dezvoltarea continuă a utilizării calculatoarelor în toate domeniile vieții, existența și evoluția rețelelor informatice de comunicații la nivel național și internațional, globalizarea comunicațiilor, existența unor baze de date puternice, constituie premisele societății informaționale în care trăim.

Protecția acestor sisteme, de transmitere și stocare a datelor, presupune existența unor servicii de rețea care să asigure securitatea datelor, cum ar fi :

* Confidențialitatea
* Nerepudierea
* Autenticitatea
* Controlul accesului
* Integritatea
* Disponibilitatea

**Confidențialitatea** este serviciul care are rolul de a proteja datele de atacurile pasive, adică de interceptarea datelor de persoane neautorizate. Se pot identifica mai multe nivele de protecție a acestui serviciu. Cel mai larg nivel a acestuia protejează datele transmise de toți utilizatorii unui sistem.

**Autenticitatea** este serviciul legat de garantarea autenticității comunicației. În cazul unui singur mesaj, cum ar fi un semnal de avertisment, funcția serviciului de autenticitate este de a garanta destinatarului că sursa mesajului este aceea care se pretinde a fi. În cazul unei interacțiuni, cum ar fi conectarea unui terminal la un server, două aspecte sunt implicate.

**Integritatea** este serviciul care trebuie să asigure recepționarea mesajelor așa cum au fost transmise fără copierea, inserția, modificarea, rearanjarea sau retransmiterea acestora. Acest serviciu include și protecția împotriva distrugerii datelor. El mai poate include și recuperarea datelor după un atac.

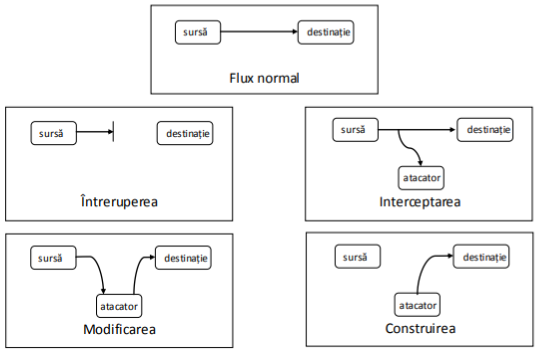
**Nerepudierea** împiedică atât expeditorul cât și destinatarul de a nega transmiterea sau recepționarea unui mesaj. Când un mesaj este trimis, destinatarul poate dovedi că mesajul a fost trimis de pretinsul expeditor.

**Controlul** accesului este abilitatea de a limita și controla accesul la sisteme gazdă și aplicații prin legături de comunicație.

**Disponibilitatea** se referă la asigurarea că sistemele de calcul sunt accesibile utilizatorilor autorizați când și unde acestia au nevoie și în forma necesară, adică informația stocată electronic este unde trebuie să fie, când trebuie să fie și în forma în care trebuie să fie.

Atacuri asupra securitații sistemelor informatice

Informația care circulă într-un sistem de transmitere și stocare a datelor are un flux normal adică de la sursă la destinație. Atacurile asupra securității sistemelor de transmitere și stocare a datelor sunt acele acțiuni care interceptează, modifică, distrug sau întârzie fluxul normal de date. O clasificare a acestor atacuri este reprezentată în figura 1 :



**Intreruperea**: O componentă a sistemului este distrusă, devine indisponibilă sau inutilizabilă total sau pentru o anumită perioadă de timp. Acest tip de atac este un atac asupra disponibilității. Exemple de astfel de atacuri ar fi: distrugerea unor echipamente hardware, tăierea liniilor de comunicație.

**Interceptarea**: Inamicul obține acces la o componentă a sistemului.

**Modificarea**: Inamicul obține nu numai acces la o componentă din sistem, dar și falsifică informația obținută. Acesta este un atac asupra integrității. Exemplele includ modificarea unor valori din fișiere de date, modificarea unor programe sau transmiterea unor mesaje false prin rețea.

**Construirea**: Inamicul pătrunde în sistem și imită unele componente din acesta. Un atac de acest tip este un atac asupra autenticității. Un exemplu de acest gen ar putea fi introducerea unor mesaje false în rețea care sunt interpretate ca mesaje reale și inventarea unor fișiere care pot induce în eroare utilizatorii reali.

# Introducere în criptografie

Criptografie = κρσπτός {kryptós} (ascuns) + γράφειν {gráfein} (a scrie)

**Criptografia** (cuvânt derivat din limba greacă a cuvintelor kryptós și gráfein reprezentând scriere ascunsă) este știința care se ocupă cu studiul codurilor și cifrurilor. Un cifru este de fapt un algoritm criptografic care poate fi folosit pentru a transforma un mesaj clar (text clar) într-un mesaj indescifrabil (text cifrat). Acest proces de transformare se numește criptare iar procesul invers se numește decriptare. Textul cifrat poate fi transmis ulterior prin orice canal de comunicații fără a ne face griji că informații sensibile ar putea ajunge în mâinile inamicilor.

Știința care se ocupă cu decriptarea (spargerea) cifrurilor se numește criptanaliză. Criptanaliza se ocupă cu studiul transformării unui text neinteligibil înapoi în cel inteligibil fără a cunoaşte cheia de criptare.

Sistemul format dintr-un algoritm de criptare și o cheie de criptare se numește criptosistem.

Inițial, securitatea unui cifru depindea de faptul că inamicul nu cunoștea algoritmul de criptare folosit, dar pe măsură ce criptografia a evoluat, securitatea cifrului s-a bazat pe utilizarea unei chei secrete care se poate extrage din textul cifrat. Până la jumătatea secolului XX, nu a fost demonstrat faptul că un anumit cifru nu poate fi spart, ba chiar întreaga istorie a criptografiei este plină de relatări în care anumit cifru era spart iar ulterior erau creați alți algoritmi care la rândul lor erau sparți.

# Criptografia clasică

Toate criptosistemele pot fi impărțite în două tipuri: criptosisteme simetrice numite și clasice sau convenționale și criptosisteme asimetrice numite și moderne. Criptosistemele simetrice, sau cu cheie secretă, sunt acele criptosisteme în care numai emițătorul și receptorul cunosc cheia secretă pe care o aplică la fiecare criptare sau decriptare.

Criptosistemele asimetrice, sau cu cheie publică, se bazează pe perechi de chei. Una din chei (cheia publică) este folosită la criptare, iar celaltă (cheia privată) este folosită la decriptare.

În criptografia clasică mesajul clar, numit şi text clar, este convertit într-o secvență aparent aleatoare şi fără sens, numită text cifrat. Procesul de criptare presupune un algoritm de criptare şi o cheie de criptare.

Această cheie este o valoare independentă de textul care se doreşte a fi criptat. Odată produs, textul criptat trebuie transmis destinatarului. La recepție acest text criptat trebuie transformat în textul original folosind un algoritm de decriptare bazat pe aceeaşi cheie folosită la criptare.

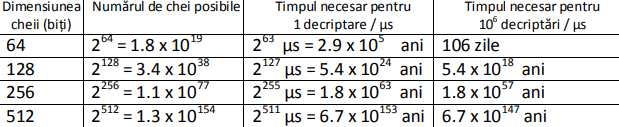
## Securitatea criptării clasice

Securitatea criptării convenționale depinde de două aspecte esențiale: algoritmul de criptare și cheia de criptare. Algoritmul de criptare, care trebuie să fie destul de puternic pentru a face imposibilă o decriptare numai pe baza textului criptat.

Există două cerințe esențiale care trebuie să le îndeplinească un **algoritm de criptare** :

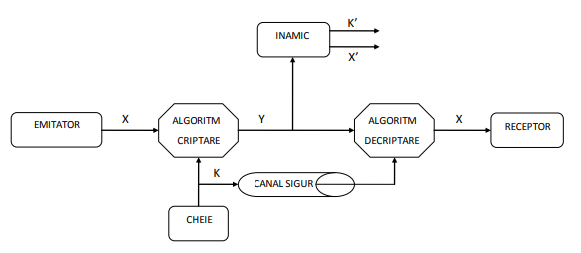
1. Costul spargerii codului să depășească valoarea informației criptate;
2. Timpul necesar spargerii codului să depășească timpul de viață al informației, adică timpul până când informația are valoare.

Un algoritm de criptare care satisface aceste două cerințe este numit algoritm cu securitate computațională. Prezentăm în tabelul 1, cât timp este necesar pentru a decripta un text cifrat, folosind metoda forței brute (brute force), pentru diferite dimensiuni ale cheii de criptare.



## Modelul criptării clasice

Un model de criptosistem simetric (clasic) este prezentat în figura 2.



## Criptografia modernă

Un criptosistem asimetric care deocamdată este considerat a fi sigur poate fi implementat folosind algoritmul RSA [5], creat în 1978 de către Ronald Rivest, Adi Shamir și Leonard Adleman. Algoritmul RSA este folosit în prezent pentru securizarea comunicațiilor din internet, a tranzacțiilor bancare sau a comerțului electronic.

Securitatea lui se bazează pe complexitatea matematică pe care o impune factorizarea numerelor prime. Pentru securizarea comunicațiilor, guvernul Statelor Unite folosește algoritmul AES (Advanced Encryption Standard) [8], dezvoltat de către Joan Daemen și Vincent Rijmen și acceptat ca standard de către NIST (National Institute of Standards and Technology) în anul 2001.

Algoritmul AES este un cifru bloc (128 biți) simetric capabil să cripteze sau să decripteze informația folosind chei criptografice pe 128,192, respectiv 256 de biți. AES se remarcă prin simplitate și prin performanțe criptografice ridicate, fiind ușor de implementat atât software cât și hardware. Deci, criptosistemele cu chei publice suplinesc dezavantajul major al celor cu cheie secretă datorită faptului că nu mai este necesar schimbul de chei.

Totuși, criptosistemele RSA și AES au marele inconvenient că securitatea lor se bazează pe complexitatea matematică a calculelor; în funcție de dimensiunea cheii folosite, pentru decriptare pot fi necesari și câteva mii de ani, la puterea de calcul actuală. Având în vedere faptul că, încă din 1985, David Deutsch a descris principiile de funcționare ale unui calculator cuantic [9] – un supercalculator cu o putere de calcul extraordinar de mare care funcționează pe principiile fizicii cuantice, putem presupune că în viitor criptosistemele cu chei publice ar putea deveni nesigure.

În concluzie, singurul criptosistem absolut sigur rămâne one-time pad. Problema schimbului de chei poate fi rezolvată printr-un sistem de distribuire a cheilor cuantice (QKD – Quantum Key Distribuiton).