Dominic M. Kristály

# Criptografie

## - Notițe de curs -

EDITURA UNIVERSITĂȚII TRANSILVANIA DIN BRAȘOV

Brașov, 2023

# Cuprins


**1. SECURITATEA INFORMAȚIILOR DIGITALE. COMPONENTE ... 3**

**2. CRIPTOGRAFIA ... 6**

2.1. CRIPTOGRAFIA ÎN ISTORIE ... 6

**3. SISTEME CRIPTOGRAFICE CLASICE ... 8**

3.1. CIFRURI CLASICE ... 8

*3.1.1. Cifrul de substituție mono-alfabetică ... 8*

*3.1.2. Cifrul de substituție poli-alfabetică ... 9*

*3.1.3. Cifrul de transpoziție ... 9*

*3.1.4. Cifrul poligramic ... 9*

3.2. CIFRURI DE SUBSTITUȚIE MONO-ALFABETICĂ ... 9

*3.2.1. Cifrul Cezar ... 9*

3.3. CIFRURI DE SUBSTITUȚIE POLI-ALFABETIC ... 10

*3.3.1. Cifrul Vigenère ... 10*

*3.3.2. Cifrul Beaufort ... 10*

*3.3.3. Cifrul Autokey ... 10*

3.4. CIFRURI DE TRANSPOZIȚIE ... 11

*3.4.1. Cifrul Route ... 11*

3.5. CIFRUL PLAYFAIR ... 12

3.6. CIFRUL VERNAM ... 13

**4. SISTEME ȘI FUNCȚII CRIPTOGRAFICE ... 15**

4.1. PROTOCOL CRIPTOGRAFIC ... 16

4.2. CRIPTOSISTEME ... 17

**5. SISTEME CRIPTOGRAFICE SIMETRICE ... 19**

5.1. OPERAȚII UNIVERSALE UTILIZATE ÎN CRIPTAREA SIMETRICĂ ... 20

*5.1.1. Substituția ... 20*

*5.1.2. Transpoziția ... 20*

5.2. OPERAȚIA SAU EXCLUSIV (XOR) ÎN CRIPTOGRAFIE ... 20

5.3. TIPURI DE CODURI ... 21

*5.3.1. Coduri bloc ... 21*

*5.3.2. Coduri flux ... 21*

5.4. CODURI FLUX SINCRONE ... 22

5.5. CODURI FLUX CU AUTOSINCRONIZARE ... 22

5.6. MODURI DE OPERARE A CODURILOR DE TIP BLOC ... 23

*5.6.1. Electronic Codebook (ECB) ... 23*

*5.6.2. Cipher Block Chaining (CBC) ... 24*

*5.6.3. Cipher Feedback (CFB) ... 24*

*5.6.4. Output Feedback (OFB) ... 25*

*5.6.5. Counter (CTR) ... 26*

*5.6.6. ECB versus CBC ... 26*

5.7. SCHEME DE COMPLETARE A BLOCURILOR (PADDING) ... 28

5.8. ALGORITMUL AES ... 28

*Pasul SubBytes* ..... *29*
*Pasul ShiftRows* ..... *30*
*Pasul MixColumns* ..... *30*
*Pasul AddRoundKey și planificarea cheilor* ..... *31*
5.9. COMPARAȚIE ÎNTRE ALGORITMII CRIPTOGRAFICI SIMETRICI ..... 32
**6. SISTEME CRIPTOGRAFICE ASIMETRICE ..... 36**
6.1. ALGORITMUL RSA ..... 38
**7. FUNCȚII IREVERSIBILE ..... 39**
7.1. FUNCȚII IREVERSIBILE DE TIP HASH ..... 39
7.2. CODURI DE IDENTIFICARE A MESAJELOR ..... 41
**8. CRIPTOSISTEME HIBRIDE ..... 42**
**9. STEGANOGRAFIA ..... 44**
9.1. STEGANOGRAFIA DIGITALĂ. TEHNICA LSB ..... 45
9.2. UTILIZAREA TEHNICII LSB PENTRU ASCUNDEREA MESAJELOR ÎN FIȘIERE BITMAP ..... 45
9.3. UTILIZAREA TEHNICII LSB PENTRU ASCUNDEREA MESAJELOR ÎN FIȘIERE H.264 ..... 47
**10. SECURIZAREA CANALELOR DE COMUNICAȚIE ..... 51**
**BIBLIOGRAFIE ..... 52**

# 1. Securitatea informațiilor digitale. Componente

Protecția informațiilor personale sau restricționate publicului larg este un subiect de mare interes în societatea informațională în care trăim. Informația este un activ al unei organizații care prezintă o importanță deosebită și, în consecință, necesită o protecție adecvată. Informațiile pot exista sub diferite forme: tipărite sau scrise pe hârtie, stocate electronic, transmise prin poștă sau prin echipamente electronice, prezentate în filme sau comunicate în cadrul unor conversații. Orice formă ar avea informațiile sau orice metode de stocare ar fi folosite, ele trebuie să fie întotdeauna protejate corespunzător. Securitatea informațiilor își propune să asigure **confidențialitatea**, **integritatea**, **disponibilitatea** și **nerepudierea** informațiilor, prin protejarea acestora de o gamă largă de amenințări și vulnerabilități, având ca obiectiv continuitatea activității și minimalizarea riscurilor.

Semnificațiile componentelor securității informațiilor sunt următoarele:

- **Confidențialitatea** asigură că informația este accesibilă doar entităților care sunt autorizate să aibă acces la resursă. Pentru asigurarea confidențialității trebuie identificate toate informațiile care trebuie protejate, precum și proprietarul acestora și persoanele care trebuie să aibă acces la ele. Asigurarea confidențialității implică o serie de măsuri standardizate de protecție împotriva accesului neautorizat la date și informații.

- **Integritatea** își propune protejarea corectitudinii și caracterului complet al informației și metodelor de procesare. Asigurarea integrității datelor și informațiilor presupune implementarea unui set de măsuri adecvate, care să nu permită alterarea/modificarea sau distrugerea informațiilor de către persoane rău intenționate. Măsurile de control instituite trebuie să definească utilizatorii care au drept de acces și de modificare asupra informațiilor, precum și metodele și mijloacele de recuperare a informațiilor în cazul distrugerii sau pierderii acestora ca urmare a unei erori hardware, software, erori umane sau a unei erori a sistemelor de securitate.

- **Disponibilitatea** își propune să asigure accesul utilizatorilor autorizați la informații și la bunurile asociate atunci când le sunt necesare.

- **Nerepudierea** este o componentă mai nouă a securității informațiilor care își propune să confirme destinatarului unui mesaj electronic faptul că acest mesaj este scris și trimis de o anumită persoană, care nu poate nega emiterea acestuia. [IPSS]

Securitatea informațiilor este obținută prin implementarea unui set adecvat de măsuri de securitate, printre care se numără politici, procese, proceduri, structuri organizaționale și funcțiuni legate de software și hardware. Aceste măsuri de securitate trebuie stabilite, implementate,

monitorizate, analizate și îmbunătățite, când este cazul, pentru a se asigura atingerea obiectivelor stabilite de securitate.

În general, amenințările la adresa informațiilor sunt generate de **cauze umane** (erori, neglijență, *hacking*, *cracking*, *phishing*, software malițios, sabotaj, spionaj, terorism etc), **cauze legate de costuri** (procese inadecvate, soluții ieftine, testări insuficiente etc), **cauze tehnice** (hardware, software), **cauze externe** (dezastre naturale - foc, apă, cutremur, incidente, accidente, terorism etc).

Amenințările pot fi accidentale sau intenționate. Amenințările **accidentale** sunt acele amenințări care se realizează fără o intenție premeditată. Exemple de amenințări accidentale sunt disfuncționalitățile sistemului, programele cu erori și operările greșite. Amenințările **intenționate**, dacă sunt realizate, atunci ele sunt considerate *atacuri*.

Funcție de locul de manifestare, amenințările pot fi grupate în interne și externe. Amenințările **interne** vin din partea propriilor angajați, ori sunt cauzate de disfuncții ori neconformități în funcționarea sistemelor, iar amenințările **externe** vin din partea foștilor angajați, agenților de spionaj, teroriștilor, hackerilor etc. Întotdeauna o amenințare exploatează o *vulnerabilitate* existentă la nivelul unei resurse informaționale.

**Vulnerabilitățile** sunt slăbiciuni asociate resurselor (specifice mediului fizic, personalului, managementului, administrației, resurselor hardware, software, comunicații etc.), care pot cauza daune numai dacă sunt exploatate de amenințări.

La modul general, vulnerabilitățile unui sistem pot fi:

- **vulnerabilități de proiectare**, cauzate de slăbiciunile de proiectare ale sistemului;
- **vulnerabilități forțate**, cauzate de restricții sau cerințe externe sistemului, cum ar fi cerințele pentru interceptarea legală a comunicațiilor și pentru protecția datelor cu caracter personal;
- **vulnerabilități evitabile**, cauzate de o proprietate fundamentală a sistemului și care pot fi protejate complet printr-o anumită caracteristică de securitate;
- **vulnerabilități inevitabile**, cauzate de către o funcție sensibilă a sistemului și pentru care nu se poate găsi o soluție de securizare.

Exemple concrete de vulnerabilități: linii de comunicație neprotejate, (vulnerabilitate ce poate fi exploatată de amenințarea de interceptare a comunicațiilor); puncte de conexiune neprotejate (infiltrare comunicații); lipsa mecanismelor de identificare și autentificare (substituire de identitate); transferul parolelor în clar (accesare rețea de utilizatori neautorizați); linii dial-up (accesare rețea de utilizatori neautorizați); administrare neadecvată a rețelei (supraîncărcare

trafic); interfață de utilizator complicată (eroare de utilizator); lipsa unei proceduri de ștergere a mediilor de stocare înainte de reutilizare (utilizare neautorizată software); lipsa unui control adecvat al modificărilor (defecțiuni software); administrare defectuoasă a parolelor (substituire identitate).

Exploatarea unei vulnerabilități de către o amenințare conduce la un risc, care trebuie evaluat și cuantificat. [OPRE] [IPSS]

**Riscul** reprezintă o pagubă (pierdere) potențială pentru o organizație, în situația când o amenințare exploatează o vulnerabilitate și este exprimat cel mai bine prin răspunsul la următoarele întrebări:

- ce se poate întâmpla (care este amenințarea)?
- care este impactul sau consecința?
- care este frecvența (cât de des se poate întâmpla)?

# 2. Criptografia

Criptografia reprezintă arta protejării informațiilor prin transformarea lor într-o formă ininteligibilă pentru cei care nu dețin secretul de decriptare corespunzătoare (**cheia**).

Criptografia joacă un rol fundamental în asigurarea securității în era digitală în care trăim. Ea își are originile în antichitate, fiind folosită inițial pentru a proteja mesajele secrete transmise între conducători și diplomați. Cu toate acestea, odată cu avansul tehnologiei, criptografia a evoluat semnificativ, dezvoltându-se într-un domeniu complex și sofisticat care influențează aproape toate aspectele vieții noastre digitale.

Principala idee din spatele criptografiei constă în transformarea datelor într-o formă ilizibilă pentru persoanele neautorizate. Aceasta se realizează cu ajutorul algoritmilor matematici special creați pentru acest scop. Există două tipuri principale de criptare: criptarea simetrică și criptarea asimetrică. În criptografia simetrică, aceeași cheie este folosită atât pentru criptare, cât și pentru decriptare. În schimb, în criptografia asimetrică, se folosesc două chei diferite: una pentru criptare și alta pentru decriptare. Acest ultim tip de criptare a fost revoluționar în asigurarea schimbului securizat de informații pe internet și în autentificarea digitală.

Criptografia nu se limitează doar la protejarea datelor sensibile. Ea este prezentă într-o varietate de aplicații, de la securitatea tranzacțiilor financiare online până la autentificarea în sistemele informatice sau protejarea intimității utilizatorilor. În plus, criptografia joacă un rol crucial în dezvoltarea tehnologiilor emergente precum blockchain și criptomonede, asigurând integritatea și confidențialitatea tranzacțiilor digitale.

Cuvântul *criptografie* derivă din limba greacă veche, din termenul *kryptós*, care înseamnă "ascuns" sau "secret", și *gráphein*, care se traduce ca "a scrie". Împreună, aceste două cuvinte definesc conceptul de a scrie într-un mod secret sau ascuns, dezvoltându-se în ceea ce astăzi numim criptografie - arta și știința de a proteja informațiile prin transformarea lor într-o formă ininteligibilă pentru cei care nu dețin cheia corectă pentru decriptare.

## 2.1. Criptografia în istorie

În antichitate, criptografia a jucat un rol crucial în securizarea comunicării și în protejarea informațiilor sensibile. Unul dintre cele mai vechi exemple de criptare provine din Egiptul antic, unde se folosea "cifrul substituție" pentru a ascunde mesajele. În acest caz, literele din mesaj erau înlocuite cu alte litere, cifre sau simboluri într-un mod prestabilit.

Un exemplu notabil este cifrul numit "cifrul Cezar", numit astfel datorită utilizării de către Iulius Cezar. Acesta presupunea înlocuirea fiecărei litere din mesaj cu litera situată cu un anumit număr de poziții mai departe în alfabet.

Un alt exemplu notabil provine din Grecia antică, unde se folosea "scitala" - un dispozitiv format dintr-un băț în jurul căruia se înfășurau benzi de pergament (Figura 2.1). Mesajul era scris pe benzile înfășurate și, când benzile erau desfăcute și așezate în ordinea corectă pe o altă scitală similară deținută de destinatar, mesajul real devenea vizibil.

**Figura 2.1 - Scitala (*Wikimedia Commons*)**

În China, se folosea criptarea prin substituție, unde caracterele erau înlocuite cu alte caractere sau simboluri într-un mod secret. Uneori, chiar se foloseau caractere sau cuvinte care aveau sens, dar nu direct legat de mesajul real, pentru a confunda eventualii interceptori.

# 3. Sisteme criptografice clasice

Criptografia, ca domeniu al securității informației, a cunoscut diverse evoluții și transformări de-a lungul timpului. Înainte de era digitală, toate criptosistemele se bazau pe scheme de criptare cu chei simetrice, unde atât procesul de criptare, cât și cel de decriptare, foloseau aceeași informație - cheia. Aceste sisteme reprezentau un pas important în direcția protejării informațiilor sensibile, oferind în primul rând **confidențialitate**.

Deși erau limitate în ceea ce privește serviciile de securitate pe care le ofereau, adică se concentrau în principal pe păstrarea secretului comunicațiilor, aceste criptosisteme clasice au avut un impact semnificativ în istoria criptografiei. Ele au fost fundamentele pe care s-au dezvoltat tehnologiile ulterioare, încurajând cercetarea în direcția găsirii unor metode mai sofisticate și eficiente de protejare a datelor.

Un aspect distinctiv al criptosistemelor clasice este faptul că acestea operau într-un context analitic diferit față de sistemele moderne. În timp ce criptosistemele moderne, digitale, utilizează datele ca numere binare și aplică algoritmi matematici complecși, cele clasice se bazau pe alfabete sau simboluri ca elemente de bază. Aceasta a avut un impact semnificativ asupra modului în care mesajele erau criptate și decriptate, întrucât operațiile se bazau pe permutări și substituții de simboluri.

Un element esențial în orice criptosistem clasic este **cifrul**. Cifrul reprezintă un set de pași sau un algoritm bine definit, care descrie procesul de criptare și decriptare. Acest algoritm își propune să transforme mesajul original într-o formă ininteligibilă în funcție de o cheie specifică, iar destinatarul, deținând cheia corespunzătoare, poate reveni la forma inițială a mesajului. Aceasta presupune ca părțile participante să cunoască a-priori această cheie (secret).

## 3.1. Cifruri clasice

Cifrurile clasice reprezintă o varietate de tehnici de criptare utilizate în istoria criptografiei, înaintea dezvoltării tehnologiilor digitale. Aceste cifruri au pus bazele și au influențat evoluția ulterioară a securității cibernetice. Iată câteva tipuri reprezentative de cifruri clasice:

### *3.1.1. Cifrul de substituție mono-alfabetică*

Acest tip de cifru implică înlocuirea fiecărei litere sau simbol din textul simplu cu un alt simbol, în conformitate cu o regulă de substituție specifică. Un exemplu este "Cifrul Cezar", unde fiecare literă este deplasată cu un anumit număr de poziții în alfabet.

### *3.1.2. Cifrul de substituție poli-alfabetică*

În acest caz, un singur simbol din textul simplu poate fi înlocuit cu mai multe simboluri din textul cifrat, în funcție de poziția sa în cuvânt sau în mesaj. Cifrul Vigenère este un exemplu notabil de cifru poli-alfabetic, unde cheia determină modul de substituție pentru fiecare literă.

### *3.1.3. Cifrul de transpoziție*

În loc să înlocuiască simbolurile cu altele, cifrurile de transpoziție reorganizează ordinea simbolurilor pentru a crea textul cifrat. Mesajul este scris într-o matrice și apoi este citit într-un mod specific, de obicei în linii sau coloane, pentru a obține textul cifrat. Un exemplu este cifrul "Scitala".

### *3.1.4. Cifrul poligramic*

Cifrul poligramic implică înlocuirea perechilor de litere consecutive (digrame) sau a grupurilor de litere (trigrame) cu alte perechi sau grupuri de litere dintr-un set predefinit. Aceasta adaugă un nivel suplimentar de complexitate în procesul de criptare.

## 3.2. Cifruri de substituție mono-alfabetică

Cifrurile de substituție mono-alfabetică reprezintă o categorie de tehnici criptografice în care fiecare literă sau simbol din textul simplu este înlocuit cu un alt simbol sau literă pentru a forma textul cifrat. Acest tip de cifru este una dintre primele și cele mai simple modalități de a cripta informații și a asigura confidențialitatea mesajelor. Deși cifrurile mono-alfabetice sunt relativ simple, ele au jucat un rol esențial în dezvoltarea criptografiei și înțelegerea conceptelor de bază ale securității cibernetice.

Un exemplu notabil de cifru mono-alfabetic este "Cifrul Caesar", numit după Iulius Cezar, care se spune că l-ar fi folosit pentru a proteja mesajele militare. În acest cifru, fiecare literă din textul simplu este înlocuită cu o altă literă, unde substituția se bazează pe o deplasare constantă a literelor în alfabet. Acest lucru face ca mesajul să fie relativ ușor de decriptat, mai ales cu ajutorul tehnicilor moderne de analiză statistică.

### *3.2.1. Cifrul Cezar*

Unul dintre cele mai vechi și simple tipuri de cifru mono-alfabetic este **cifrul de deplasare**, adesea cunoscut sub numele de "Cifrul Cezar". Acesta reprezintă o formă rudimentară de schemă de substituție, în care fiecare literă a textului simplu este înlocuită cu o altă literă din alfabet pentru a crea textul cifrat. Conceptul de bază constă în a schimba fiecare simbol (literă sau caracter) cu un alt simbol care este "deplasat" în alfabet cu un număr fix între 0 și 25.

Pentru exemplificare, dacă alegem o deplasare de 3, litera A ar fi înlocuită cu litera D, litera B cu litera E, și tot așa. Atât expeditorul, cât și destinatarul trebuie să fie de acord asupra unui "număr