Universitatea Tehnică a Moldovei

# ANALIZA COMPARATIVĂ A EFICACITĂȚII SISTEMELOR SIMETRICE DE CRIPTARE

**Student:** **Muntean Eduard**

**Coordonator:** **Cerbu Olga**
**conf. univ., Dr.**

**Chișinău, 2023**

**MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA**
**Universitatea Tehnică a Moldovei**
**Facultatea Electronică și Telecomunicații**
**Departamentul Telecomunicații și Sisteme Electronice**

**Admis la susținere**
**Șef department TSE:**
**Sava Lilia, conf.univ.dr.**
**_____**
**"___" _____ 2023**

# ANALIZA COMPARATIVĂ A EFICACITĂȚII SISTEMELOR SIMETRICE DE CRIPTARE

## Teză de master

**Student:** _____ **Muntean Eduard, Gr. SISRC-211M.**
**Coordonator:** _____ **Cerbu Olga, Conf.univ.dr.**

**Chișinău, 2023**

# REZUMAT

**Autor:** Muntean Eduard, gr. SISRC-211M.

**Tema:** "Analiza comparativă a eficacității sistemelor simetrice de criptare"

**Structura lucrării:** constă din titlu, aviz, rezumat, introducere, 3 capitole, concluzii, bibliografie, anexe.

**Cuvinte-cheie:** criptare, securitatea informației, criptoanaliză, standard.

**Problematica studiului:** Analiza sistemelor de criptare simetrică bazata pe blocuri cu cheie secretă a elementelor de criptoanaliză diferențială și liniare cât și implementarea într-un limbaj de programare a unor sisteme simetrice.

**Scopul lucrării:** Analiza comparativă a eficacității sistemelor simetrice de criptare.

**Obiectivele lucrării:**

1. Descrierea algoritmilor criptografici ce procesează grupuri de biți de lungime fixă ale mesajului, folosind o transformare inversabilă, specificată în baza cheii secrete;
2. Descrierea sistemelor de criptare bazate pe blocuri, pe fluxuri de biți cât și modificările lor după dimensiunile cheilor, implementate într-un limbaj de programare;
3. Aplicarea rețelelor Feistel, a cifrului Feistel pentru difuzia asociată cu dependenţa biţilor de la ieşire cu biţii de la intrare;
4. Cercetarea criptanalizei diferențiale a sistemelor simetrice pentru a le oferi caracteristicile de securitate necesare;
5. Evaluarea unor metode de analiză criptografică liniara pentru sistemele de criptare cu cheie simetrică (cifrurile fluide și cifrurile bloc);
6. Efectuarea analizei compararative dintre sistemele bazate pe blocuri cu cheie simetrică.

**Metodele aplicate la elaborarea lucrării**: Pentru realizarea obiectivelor lucrării a fost necesară cercetarea metodelor criptoanalizei diferențiale și liniare cât și realizarea exemplelor numerice asupra sistemelor simetrice bazate pe blocuri cu cheie secretă.

**Rezultatele obținute:** În urma cercetărilor efectuate au fost făcută analiza comparativă între sistemele simetrice, descrise atacurile tipice asupra acestor sisteme de securitate care utilizează metode de criptare simetrice cu cheie secretă, au fost implementate în limbaj de programare Java. A fost efectuatî analiza comparativă între algoritmii simetrici RC2 și DES care includ în schemă și rețeaua Feistel.

## SUMMARY

**Author:** Muntean Eduard, gr. SISRC-211M.

**Title:** "Comparative analysis of the effectiveness of symmetric encryption systems."

**Thesis structure:** consists of title, notice, summary, introduction, 3 chapters, conclusions, bibliography, annexes.

**Keywords:** encryption, information security, cryptanalysis, standard

**Research area:** Analysis of symmetric encryption systems based on secret-key blocks of differential and linear cryptanalysis elements as well as implementation in a programming language of symmetric systems.

**Thesis purpose:** Comparative analysis of the effectiveness of symmetric encryption systems.

**Objectives:**

1. Description of cryptographic algorithms that process groups of fixed-length bits of the message using an invertible transformation, specified on the basis of the secret key;
2. Description of block-based, bit-stream based encryption systems and their key-size modifications implemented in a programming language;
3. Application of Feistel networks, Feistel cipher for diffusion associated with the dependence of output bits on input bits;
4. Investigation of differential cryptanalysis of symmetric systems to provide them with necessary security features;
5. Evaluation of linear cryptographic analysis methods for symmetric key encryption systems (fluid ciphers and block ciphers);
6. Perform comparative analysis between symmetric key block-based systems.

**Applied methods:** In order to achieve the objectives of the paper it was necessary to investigate the methods of differential and linear cryptanalysis as well as to perform numerical examples on symmetric systems based on secret key blocks.

**The results obtained:** The research carried out has made a comparative analysis between symmetric systems, described typical attacks on these security systems using symmetric encryption methods with secret key, were implemented in Java programming language. Comparative analysis of RC2 and DES symmetric algorithms including the Feistel network in the scheme was performed.

**CUPRINS**

# INTRODUCERE

Societatea îmbrăţişează din ce în ce mai mult tehnologia informaţiei. Informaţia care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. Informaţia pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puţin din punct de vedere funcţional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil şi un mijloc de comunicare prin tehnologii precum poşta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecţia informaţiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informaţiei gestionată de sistemele informatice în noul context tehnologic.

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităţilor de inscripţionat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată. Asigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Este important ca organizaţiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaţilor a importanţei securităţii informaţiilor, înţelegerea tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi aplicarea practicilor de control.

Organizaţia Internaţionala pentru Standardizare (ISO) împreuna cu Comisia Internaţională Electrotehnică (IEC) alcătuiesc un forum specializat pentru standardizare.

Organismele naţionale care sunt membre ale ISO şi IEC participă la dezvoltarea standardelor internaţionale prin intermediul comitetelor tehnice. [1]

Criptografia este știința păstrării informațiilor în siguranță, transformându-le într-o formă pe care destinatarii neintenționați nu o pot înțelege. În criptografie, un mesaj original lizibil de către om, denumit text simplu, este schimbat prin intermediul unui algoritm, sau a unei serii de operații matematice. Criptografie în securitatea rețelei a fost formarea primelor rețele de calculatoare care au început civilii să se gândească la importanța criptografiei. Calculatoarele vorbeau între ele prin rețeaua deschisă, nu doar prin conexiuni directe între ele; acest tip de rețea a fost transformator în multe moduri grozave, dar a făcut, de asemenea, ușor de cercetat datele care călătoresc prin rețea. Și serviciile financiare fiind un caz de utilizare timpurie pentru comunicarea computerizată, a fost necesar să se găsească o modalitate de a păstra informațiile secrete. În imaginea de ansamblu, totuși, există câteva obiective generale de securitate cibernetică pe care le folosim criptografiei pentru a ne ajuta să le realizăm, așa cum explică consultantul în securitate cibernetică Gary Kessler. Folosind tehnici criptografice, profesioniștii în securitate pot:

-Păstra confidențialitatea conținutului datelor;

-Autentifica identitatea expeditorului și a destinatarului unui mesaj;

-Asigura integritatea datelor, arătând că nu au fost modificate;

-Demonstra că presupusul expeditor a trimis cu adevărat acest mesaj, un principiu cunoscut sub numele de non-respingere.

Criptografia cheii secrete, uneori numită și cheie simetrică, este folosită pe scară largă pentru a păstra confidențialitatea datelor. Poate fi foarte util pentru păstrarea unui hard disk local privat, de exemplu; deoarece același utilizator criptează și decriptează în general datele protejate, partajarea cheii secrete nu este o problemă. Criptografia cu cheie secretă poate fi utilizată și pentru a păstra confidențialitatea mesajelor transmise pe internet. [17]

Tehnicile de criptare sunt utilizate în multe portofele de criptomonede ca o modalitate de a oferi niveluri sporite de securitate pentru utilizatorii finali. Algoritmii de criptare sunt aplicați, de exemplu, atunci când utilizatorii configurează o parolă pentru portofelele cripto, ceea ce înseamnă că fișierul folosit pentru a accesa software-ul a fost criptat. Cu toate acestea, datorită faptului că Bitcoin și alte criptomonede folosesc perechi de chei public-private, există o concepție greșită comună că sistemele blockchain folosesc algoritmi de criptare asimetrici. După cum am menționat anterior, criptarea asimetrică și semnăturile digitale reprezintă două cazuri majore de utilizare a criptografiei asimetrice (criptografia cu cheie publică). Prin urmare, nu toate sistemele de semnătură digitală folosesc tehnici de criptare, chiar dacă prezintă o cheie publică și una privată. De fapt, un mesaj poate fi semnat digital fără a fi criptat. RSA este un exemplu de algoritm care poate fi folosit pentru semnarea mesajelor criptate, dar algoritmul de semnătură digitală folosit de Bitcoin (numit ECDSA) nu folosește deloc criptarea. Atât criptarea simetrică, cât și cea asimetrică joacă un rol important în menținerea în siguranță a informațiilor și

comunicațiilor sensibile în lumea de astăzi dependentă de digital. Deși ambele pot fi utile, fiecare are propriile avantaje și dezavantaje și, prin urmare, sunt aplicate diferit. Pe măsură ce știința criptografiei continuă să evolueze pentru a se apăra împotriva amenințărilor mai noi și mai sofisticate, sistemele criptografice simetrice și asimetrice vor rămâne probabil relevante pentru securitatea computerelor. [18]

**Scopul lucrării:** Analiza comparativă a eficacității sistemelor simetrice de criptare.

**Obiectivele lucrării:**

1. Descrierea algoritmilor criptografici ce procesează grupuri de biți de lungime fixă ale mesajului, folosind o transformare inversabilă, specificată în baza cheii secrete;

2. Descrierea sistemelor de criptare bazate pe blocuri, pe fluxuri de biți cât și modificările lor după dimensiunile cheilor, implementate într-un limbaj de programare;

3. Aplicarea rețelelor Feistel, a cifrului Feistel pentru difuzia asociată cu dependența biţilor de la ieşire cu biţii de la intrare;

4. Cercetarea criptanalizei diferențiale a sistemelor simetrice pentru a le oferi caracteristicile de securitate necesare;

5. Evaluarea unor metode de analiză criptografică liniara pentru sistemele de criptare cu cheie simetrică (cifrurile fluide și cifrurile bloc);

6. Efectuarea analizei compararative dintre sistemele bazate pe blocuri cu cheie simetrică.

# CONCLUZII

În cadrul lucrării date am avut ca scop analiza comparativă a eficacității sistemelor simetrice de criptare. În primul capitol am descris și analizat sistemele simetrice de criptare. Nu există încă un sistem criptografic despre care se poate spune că este pe deplin sigur, însă în urma cercetărilor am constatat că algoritmii simetrici sunt mult mai eficienți în comparație cu algoritmii asimetrici. Acești algoritmi sunt, în general, de natură foarte rapidă, motiv pentru care sunt folosiți atunci când este nevoie de criptare în cantități mari de date.

Pentru atingerea scopului expus pentru realizare, analiza comparativă a eficacității sistemelor simetrice de criptare au fost îndeplinite cu succes toate obiectivele lucrării. Pentru compararea eficacității sistemelor criptografice au fost cercetate unele proprietăți efective demonstrabile ale acestora.

1. Descrierea algoritmilor criptografici ce procesează grupuri de biți de lungime fixă ale mesajului. Au fost prezentați algoritmi care folosesc transformări inversabile, specificate în baza cheii secrete;

2. Descrierea sistemelor de criptare bazate pe blocuri, pe fluxuri de biți cat și modicările lor după dimensiunile cheilor, implementare într-un limbaj de programare;

În lucrare au fost descrise multiple sisteme de criptare simetrice în care se utilizează operații de permutare, transpoziționare, operații XOR, care la rândul lor măresc eficacitatea sistemului.

3. Aplicarea rețelelor Feistel, a cifrului Feistel pentru difuzia asociată cu dependența biților de la ieșire cu biții de la intrare;

A fost demonstrată în lucrare eficacitatea utilizării rețelelor Feistel și implementarea schemei Feistel în cifru Feistel.

În capitolul doi am descris atacurile criptografice și criptanaliza. Criptanaliza este decriptarea și analiza codurilor, cifrelor sau a textului criptat, fără a avea acces la informația secretă necesară. Atacurile criptografice sunt concepute pentru a submina securitatea algoritmilor de criptare și utilizate pentru a încerca decriptarea datelor fără acces prealabil la cheie. Am cercetat că atacurile criptografice bazate pe forța brută sunt cele mai universale, dar și cele mai îndelungate. În final trebuie de subliniat că la elaborarea sistemelor de criptare trebuie să fie luate în consideraţie performanţele criptanalizei pentru a diminua riscurile posibile.

4. Cercetarea criptanalizei diferențiale a sistemelor simetrice pentru a le oferi caracteristicile de securitate necesare;

A fost cercetat compromisul spațiu-timp al atacurilor prin forță brută cât și detalii ale metodei de criptanaliză diferențială a sistemului de criptare DES.

5. Evaluarea unor  metode de analiză criptografică liniara pentru sistemele de criptare cu cheie simetrică (cifrurile fluide și cifrurile bloc);

Au fost explicate  metode avansate de analiza criptografică.

În capitolul trei am comparat algoritmii simetrici bazați pe blocuri. Am studiat că cifrurile bloc pot fi programate să funcționeze ca un cifru flux și reciproc. Cifrurile bloc operează asupra datelor cu transformări (fixe) asupra blocurilor de date clare. În cazul aplicațiilor practice, cifrurile bloc par mai generale, iar cifrurile flux sunt mai simplu de analizat din punct de vedere matematic. O altă diferență care am observat este aceea că cifrurile flux cifrează sau descifrează un singur cuvânt de date la un tact, deci nu sunt optime pentru implementările software. Cifrurile bloc sunt mai simplu de implementat din punct de vedere soft deoarece acestea operează cu blocuri de cuvinte de procesor deci sunt mai rapide.

6. Efectuarea analizei compararative dintre sistemele bazate pe blocuri cu cheie simetrică.

A fost efectuatî analiza comparativă între algoritmii simetrici RC2 și DES care includ în schema și rețeaua Feistel.

## BIBLIOGRAFIE


1. Popa Sorin Eugen. Securitatea sistemelor informatice. Note de curs şi aplicaţii. [citat la data de 10.10.2022]. Disponibil la: https://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf

2. Zgureanu Aureliu. Criptarea şi Securitatea Informaţiei. Note de curs. [citat la data de 12.10.2022]. Disponibil la: https://irek.ase.md/xmlui/bitstream/handle/123456789/236/Zgureanu%20A.%20Criptarea%20şi%20Securitatea%20Informaţiei.%20Note%20de%20curs.pdf?sequence=1&isAllowed=y

3. Sisteme de criptare simetrice. [citat la data de 13.10.2022]. Disponibil la: https://materiale.pvgazeta.info/utilizator-171/1-sisteme-de-criptare-simetrice.html

4. Maria Capcelea, Titu Capcelea. Criptografie și Securitatea Informației. Partea 1 Chișinău: CEP USM – Partea I-a. – 2021. – 215 p.. [citat la data de 14.10.2022]

5. United States Patent US3798359. [citat la data de 16.10.2022]. Disponibil la: https://www.freepatentsonline.com/3798359.pdf

6. Lucifer (criptografie). [citat la data de 18.10.2022]. Disponibil la: https://ro.frwiki.wiki/wiki/Lucifer_%28cryptographie%29

7. Horst Feistel. Cryptography and Computer Privacy. May 1973, Volume 228, No 5, pp. 15-23 [citat la data de 20.10.2022]. Disponibil la: https://www.apprendre-en-ligne.net/crypto/bibliotheque/feistel/

8. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022. [citat la data 07.11.202]. Disponibil: http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&isAllowed=y

9. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83. [citat la data 08.11.2022]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/JSS-1-2021_74-83_0.pdf

10. Lucifer (cifru). [citat la data de 22.10.2022]. Disponibil la: https://koaha.org/wiki/Lucifer_(cifrario)#L'algoritmo_originario

11. Introducere în Criptografie. [citat la data de 25.10.2022] . Disponibil la: https://moodle.usm.md/pluginfile.php/234490/mod_resource/content/0/TEMA%205.%20INTRODUCERE%20ÎN%20CRIPTOGRAFIE.%20Continutul%20temei.pdf

12. Atac de forță brută. [citat la data de 27.10.2022]. Disponibil la: https://ro.frwiki.wiki/wiki/Attaque_par_force_brute

13. Atac cu forță brută - Brute-force attack. [citat la data de 01.11.2022] . Disponibil la: https://wikicro.icu/wiki/Brute-force_attack#Theoretical_limits
14. Criptanaliza diferențială. [citat la data de 05.11.2022] . Disponibil la: https://ro.frwiki.wiki/wiki/Cryptanalyse_différentielle
15. Criptanaliza diferențială - Differential cryptanalysis. [citat la data de 08.11.2022]. Disponibil la: https://wikicro.icu/wiki/Differential_cryptanalysis
16. Criptanaliza liniară. [citat la data de 11.11.2022] . Disponibil la: https://ro.frwiki.wiki/wiki/Cryptanalyse_linéaire
17. Criptanaliza liniară - Linear cryptanalysis. [citat la data de 15.11.2022] . Disponibil la: https://wikicro.icu/wiki/Linear_cryptanalysis
18. Atac cu cheie asociată. [citat la data de 19.11.2022] . Disponibil la: https://ro.magtrain.pl/wiki/Related-key_attack
19. CE ESTE CRIPTOGRAFIA? CUM ALGORITMII PĂSTREAZĂ INFORMAȚIILE SECRETE ȘI SIGURE. [citat la data de 23.11.2022] . Disponibil la: https://www.openvision.ro/blog/academia-it/ce-este-criptografia-cum-algoritmii-pastreaza-informatiile-secrete-si-sigure/
20. Criptare simetrică vs. asimetrică. [citat la data de 30.11.2022] . Disponibil la: https://academy.binance.com/ro/articles/symmetric-vs-asymmetric-encryption
21. Criptografia simetrică. [citat la data de 05.12.2022] . Disponibil la: https://moodle.usm.md/pluginfile.php/234502/mod_resource/content/0/Tema%206.%20Criptografia%20simetrică.pdf
22. RC5. [citat la data de 10.12.2022] . Disponibil la: https://ru.wikipedia.org/wiki/RC5
23. Algoritmi simetrici. [citat la data de 12.12.2022] . Disponibil la: https://ro.education-wiki.com/3030971-symmetric-algorithms
24. Criptografia modernă. [citat la data de 15.12.2022] . Disponibil la: https://www.academia.edu/15170903/5_Criptografia_modernă
25. Статистические техники криптоанализа. [citat la data de 17.12.2022] . Disponibil la: https://habr.com/ru/post/533974/
26. Criptanaliza. Tehnici si rezultate, ED 2011. [citat la data de 18.12.2022] . Disponibil la: https://vdocuments.mx/criptanaliza-tehnici-si-rezultate-ed-2011.html?page=38