**CRIPTOGRAFIA ȘI CALCULATOARELE CUANTICE**

**Vladimir VOZIAN 1\*,**

*1Universitatea tehnică din Moldova, Facultatea Calculatoare Informatică și Microelectronică, licență ,Chișinău ,Moldova*

***Rezumat.*** *Criptografia și securitatea informațională reprezintă o ramură a matematicii și programării ce răspunde de asigurarea protecției informației. Se va vorbi despre particularitățile și modul de lucru a algoritmilor de criptare de azi, și cum criptografia poate fi distrusă de către calculatoarele cuantice, dar apoi reconstruită și dezvoltată iarăși de ele.*

***Summary.*** *Cryptography and information security are a branch of mathematics and programming that is responsible for ensuring the protection of information. We will talk about the peculiarities and workings of today's encryption algorithms, and how cryptography can be destroyed by quantum computers, but then rebuilt and re-developed by them.*

***Cuvinte cheie****: Criptografie , algoritm , calculator , calcule, cuantum, calculator cuantic.*

**Introducere:**

Nimic nu poate fi absolut, cât și securitatea unei informații. Aceasta este principala particularitate a criptografiei. Deci cum putem afirma ca o informație este într-adevăr protejată, ideea principală a securității informaționale este ca o informație se poate crede securizată dacă timpul și resursele cheltuite pentru obținerea informației au o valoare mai mare decât informația ascunsă. Ca exemplu informația cifrată să își piardă valoarea la momentul primirii ei de către răufăcător.

Deci principalele valori ce joacă rol sunt: resursele și timpul.

**Istoria criptografiei și criptanalizei**

Înainte de epoca modernă, criptografia se ocupa doar cu asigurarea confidențialității mesajelor (criptare) — conversia de mesaje dintr-o formă comprehensibilă într-una incomprehensibilă, și inversul acestui proces, pentru a face mesajul imposibil de înțeles pentru cei care interceptează mesajul și nu au cunoștințe secrete adiționale (anume cheia necesară pentru decriptarea mesajului). În ultimele decenii, domeniul s-a extins dincolo de problemele de confidențialitate și include, printre altele, și tehnici de verificare a integrității mesajului, autentificare a trimițătorului și receptorului, semnătură electronică, calcule securizate.

Cele mai vechi forme de scriere secretizată necesitau doar puțin mai mult decât hârtie și creion (sau unelte similare acestora), întrucât majoritatea oamenilor nu știau să citească. Creșterea alfabetizării a necesitat creșterea complexității criptografiei. Principalele tipuri clasice de cifruri sunt cifrurile cu transpoziție, care modifică ordinea literelor dintr-un mesaj (de exemplu „ajutor” devine „ojartu” într-o schemă trivială de rearanjare), și cifrurile cu substituție, care înlocuiesc sistematic litere sau grupuri de litere cu alte litere și grupuri de litere (de exemplu, „conexiune” devine „dpofyjvof” înlocuind fiecare literă cu următoarea din alfabet). Versiuni simple ale celor două tipuri de cifruri ofereau un grad mic de confidențialitate în cazul oponenților instruiți. Unul din primele cifruri cu substituție a fost Cifrul lui Cezar, în care fiecare literă din textul clar era înlocuită cu o literă aflată la un număr fix de poziții distanță de ea în alfabet. Cifrul a fost denumit astfel după Iulius Cezar despre care se spune că l-a folosit, cu o deplasare de 3, în comunicația cu generalii săi în timpul campaniilor militare.

**Criptografia modernă:**

[***Criptografia cu chei simetrice***](https://ro.wikipedia.org/wiki/Criptare#Criptarea_simetric%C4%83) se referă la metode de criptare în care atât trimițătorul cât și receptorul folosesc aceeași cheie (sau, mai rar, în care cheile sunt diferite, dar într-o relație ce la face ușor calculabile una din cealaltă). Acest tip de criptare a fost singurul cunoscut publicului larg până în 1976.

Studiul modern al cifrurilor cu chei simetrice se leagă mai ales de studiul cifrurilor pe blocuri și al cifrurilor pe flux și al aplicațiilor acestora. Un cifru pe blocuri este, într-un fel, o formă modernă de cifru polialfabetic Alberti: cifrurile pe blocuri iau la intrare un bloc de text clar și o cheie, și produc la ieșire un bloc de text cifrat de aceeași dimensiune. Deoarece mesajele sunt aproape mereu mai lungi decât un singur bloc, este necesară o metodă de unire a blocurilor succesive. S-au dezvoltat câteva astfel de metode, unele cu securitate superioară într-un aspect sau altul decât alte cifruri. Acestea se numesc *moduri de operare* și trebuie luate în calcul cu grijă la folosirea unui cifru pe blocuri într-un criptosistem.

[Data Encryption Standard](https://ro.wikipedia.org/wiki/Data_Encryption_Standard)(DES) și [Advanced Encryption Standard](https://ro.wikipedia.org/wiki/AES)(AES) sunt cifruri pe blocuri care sunt considerate standarde de criptografie de guvernul american (deși DES a fost în cele din urmă retras după adoptarea AES). În ciuda decăderii ca standard oficial, DES (mai ales în varianta triple-DES, mult mai sigură) rămâne încă popular; este folosit într-o gamă largă de aplicații, de la criptarea ATMla securitatea e-mail-urilorși accesul la distanță securizat. Multe alte cifruri pe blocuri au fost elaborate și lansate, cu diverse calități. Multe au fost sparte.

Cifrurile pe flux de date, în contrast cu cele pe blocuri, creează un flux arbitrar de material-cheie, care este combinat cu textul clar, bit cu bit sau caracter cu caracter. Într-un cifru pe flux de date, fluxul de ieșire este creat pe baza unei stări interne care se modifică pe parcursul operării cifrului. Această schimbare de stare este controlată de cheie, și, la unele cifruri, și de fluxul de text clar. RC4 este un exemplu de binecunoscut cifru pe flux.

Funcțiile hash criptografice (adesea numite *message digest*) nu folosesc neapărat chei, sunt o clasă importantă de algoritmi criptografici. Aceștia primesc date de intrare (adesea un întreg mesaj), și produc un hash scurt, de lungime fixă, sub forma unei funcții neinversabile. Pentru hash-urile bune, coliziunile (două texte clare diferite care produc același hash) sunt extrem de dificil de găsit.

[**Criptografia cu chei asimetrice**](https://ro.wikipedia.org/wiki/Criptografie_asimetric%C4%83)se bazează pe folosirea a doua chei diferite, una pentru criptare (cheia publică) și acea pentru decriptare (cheia privată). Principiul constă în faptul că oricine poate cripta informația cu cheia publică, pe care o știu toți, a proprietarului ei, dar decripta această informație poate dar proprietarul care e singurul care își deține cheia privată. Anume criptografia cu chei asimetrice este deja larg folosită în lume ți anume in mecanizme ca:

* Semnături digitale – un mesaj semnat cu cheia privata a emițătorului poate fi verificat de catre oricine, prin acces la cheia publica corespunzatoare, astfel asigurandu-se autenticitatea mesajului. RSA, DSA, ECDSA
* Criptarea cu cheie publică – un mesaj criptat cu o cheie publică nu poate fi decodificat decat folosind cheia privată corespunzătoare. Metoda este folosită pentru a asigura confidențialitatea. RSA/Diffie-Hellman/ElGamal

Criptografia asimetrica are ca avantaj o securitate de nivel mai înalt prelucrând date mari și care sunt greu de spars și decriptat fără cheia stabilită. Dar are ca dezavantaj este că acești algoritmi sunt de mii de ori mai lenți decât cele simetrice.

**Bazele criptării informației asimetrice:**

Principiul general al criptografiei asimetrice are o bază matematică solidă care o justifică această bază, rezumată și simplificată până la extrem, se bazează pe utilizarea unei probleme complexe , adică o operație matematică ușor de realizat, dar dificil de inversat, adică din rezultatul căreia este dificil să ne întoarcem la argumentele de plecare. Exemplul clasic este problema factorizării unui număr (găsirea numerelor prime care îl produc dacă se înmulțesc între ele: de exemplu, este ușor să înmulțiți 17 × 23 pentru a obține 391, mult mai dificil este de exemplu să luați în calcul numărul 377 în factorii primi 13 și 29) utilizați în primul și cel mai faimos sistem criptografic cu cheie publică: **[RSA](https://ro.wikipedia.org/wiki/RSA)** . Cunoașterea matematicii pure dezvoltate de om în ultimele secole a făcut ca factorizarea să fie din ce în ce mai eficientă, dar nimeni nu a reușit niciodată să facă acel pas care duce problema de la complex la non-complex; problema devine, așadar, de neconceput pentru numerele care depășesc o anumită dimensiune.

În prezent, pentru criptarea RSA, numerele de bază-10 sunt considerate „sigure”, având cel puțin 600 de cifre, ceea ce înseamnă chei de 2048 biți sau mai mult.

Criptografia este totuși o știință bazată pe probabilitate: problemele complexe sunt considerate complexe pe baza faptului că sute de ani de studiu nu au reușit să le rezolve rapid (amintiți-vă că există întotdeauna cel puțin un mod non-imediat de a rezolva o problemă: încercați să faceți operația directă cu toate numerele până la dimensiunea necesară; acest tip de soluție, în general, nici măcar nu este luat în considerare, deoarece timpul necesar crește dramatic odată cu dimensiunea numerelor utilizate), dar niciuna dintre problemele utilizate în criptografie are o teoremă care își dovedește complexitatea (singurul sistem criptografic dovedit este One Time Pad , dar din păcate este un sistem simetric - adică nu o cheie publică - și extrem de incomod de utilizat).

[**Calculatoarele cuantice**](https://ro.wikipedia.org/wiki/Calculator_cuantic)

Un **calculator cuantic** sau **computer cuantic**, folosește proprietățile cuantice ale materiei, cum ar fi suprapunerea și inseparabilitatea, pentru a efectua operațiuni pe date. Spre deosebire de calculatoarele clasice care efectuează operații logice folosind biți (şiruri binare, de 0 şi 1) și tranzistori, calculatoarele cuantice operează prin controlul comportamentului particulelor de qubiți, sau biți cuantici, care pot avea simultan mai multe poziţii (1 şi 0 în acelaşi timp), ceea ce înseamnă că pot procesa un număr enorm de rezultate potențiale simultan. Ca un exemplu mai simplu poate servi aruncarea unei monede, până când moneda nu va fi prinsă, ea nu are valoare fixă, așa lucrează și qubitul. Computerele cuantice sunt cotate cu un rating în ceea ce privește volumul cuantic, care ia în calcul numărul total de qubiți. Deşi există deja prototipuri de calculatoare cuantice, ele nu pot efectua în prezent decât sarcini similare cu cele realizate de un computer normal, dar mult mai rapid.

Deci principala deosebire este că ele funcționează folosind qubiții care reprezintă o cantitate de informație mai complexă ca bitul obișnuit. Apariția calculatoarelor cuantice va cauza distrugerea criptografiei și securității informaționale aplicate în ziua de azi, cât de amplu și dificil nu ar fi algoritmul de azi el va fi procesat de catre un calculator cuantic in timp de secunde. Algoritmele avansate de azi folosesc algoritme matematici ample care sunt practic unidirecționale, ușor de realizat la criptare, dar aproape imposibile la decriptare fără cheie. Cu cât mai mare numere se folosesc la criptare cu atât crește exponențial timpul și resursele necesare la decriptare.

***Internetul și programarea:***Marile companii care oferă servicii de căutare pe Internet – Google, Yahoo, Microsoft, ar putea beneficia enorm de pe urma unor algoritmi cuantici care să indexeze şi să efectueze căutări în baze de date imense mult mai rapid. De asemenea, pentru detectarea virușilor și a hackingului în rețele.

O aplicație a acestor sisteme ar fi în ***medicină***, în domeniul modelării moleculare. Una dintre cele mai promițătoare aplicații ale calculatoarelor cuantice este simularea comportamentului materiei până la nivelul molecular, cum ar fi simularea comportamentului compușilor proteici din corp, impactul și modul de funcțiune a virușilor, bacteriilor ș.a.. Companiile farmaceutice folosesc simulările cuantice pentru a analiza și compara compușii care ar putea duce la crearea de noi medicamente și de modele proteice sau pentru a îmbunătăți viteza și calitatea imaginilor medicale.

[***Inteligența artificială***](https://ro.wikipedia.org/wiki/Inteligen%C8%9B%C4%83_artificial%C4%83) poate beneficia masiv de pe urma utilizării calculatoarelor cuantice. Cele mai inteligente sisteme de învățare automată funcționează pe baza unui proces de ”trial and error” (identificarea anomaliilor statistice). Sistemele de ‘’deep’’ și ‘’machine learning’’ vor ajunge mult mai puternice și mai rapide, dacă pot profita de pe urma fenomenului de superpoziție.

***Industria auto***: Producătorii auto precum Volkswagen și Daimler folosesc calculatoare cuantice pentru a simula compoziția chimică a bateriilor vehiculelor electrice pentru a ajuta la găsirea de noi modalități de îmbunătățire a performanței lor. Volkswagen a prezentat un serviciu care calculează rutele optime pentru autobuze și taxiuri în orașe pentru a reduce la minimum congestia traficului.

***Concluzii:***

Dar calculatorul cuantic se crede a fi asa spus sabie cu două tăișuri, ele totodată vor distruge criptografia cu algoritmele ei de azi, dar va evolua datorită tehnilogiilor noi cuantice, adică se vor crea noi algoritmi mai complexe, dar calculatoarele cuantice nu vor creanconsecințe doar în sfera securității sau programării dar și în alte sfere.

**Bibliografie:**

<https://ro.wikipedia.org/wiki/Calculator_cuantic>

<https://ro.wikipedia.org/wiki/AES>

<https://ro.wikipedia.org/wiki/Data_Encryption_Standard>

<https://ro.wikipedia.org/wiki/RSA>

<https://ro.wikipedia.org/wiki/Calculator_cuantic>

<https://ro.wikipedia.org/wiki/Inteligen%C8%9B%C4%83_artificial%C4%83>

Douglas R. Stinson. Cryptography. Theory and Practice - 4th\_ed

Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, 2-nd ed