Classic Cryptography (Pre-computational)

Alin Titus PÎRCALAB

The information (religious, military, economic, etc.) always meant power, therefore the need to protect it, to make it accessible only for elite persons/groups, for initiated persons/group, was debated even from old times. In fact the history of cryptology/cryptographic follows closely the increase and decrease of large empires and civilizations. It doesn't occur and it doesn't develop only where the power is and it must be protected.
***Keywords**: cryptography, substitution cipher, rotor machine.*

Criptografia clasică este criptografia dinaintea calculatorului, de unde şi denumirea de *criptografie pre-computaţională*. În criptografia clasică, algoritmii erau bazaţi pe caracter şi constau dintr-o serie de transformări elementare (substituţii, transpoziţii) ale caracterelor textului în clar. Unii algoritmi aplicau aceste transformări în mod repetat, îmbunătăţind în acest mod securitatea algoritmului. În criptografia modernă bazată pe calculator (criptografie computaţională), lucrurile s-au complicat, dar multe dintre ideile criptografiei clasice au rămas nemodificate. Criptografia clasică se încadrează în clasa criptografiei cu chei simetrice.

Cifrul de substituţie *(substitution cipher)* este cifrul bloc la care fiecare caracter sau grup de caractere ale textului în clar (M) este substituit cu un alt caracter sau grup de caractere în textul cifrat (C), descifrarea făcându-se prin aplicarea substituţiei inverse asupra textului cifrat. În criptografia clasică există patru tipuri de cifruri de substituţie.

1) *Cifruri de substituţie monoalfabetică (monoalphabetic ciphers)* sunt cifrurile în care fiecare caracter al textului în clar (M) este înlocuit cu un caracter corespondent în textul cifrat (C). Vom aminti câteva dintre cifrurile de substituţie cele mai cunoscute:

A. Cifrul lui Cesar este un cifru cu substituţie monoalfabetică:

- fiecare literă a textului în clar este înlocuită cu o nouă literă obţinută printr-o deplasare alfabetică;
- cheia (aceeaşi la criptare cât şi la decriptare) constă în numărul care indică deplasarea alfabetică **C = aM + b (mod N)** unde *a* se numeşte factor de amplificare, iar b coeficient de deplasare.

Făcând corespondenţa biunivocă între literele alfabetului latin (N=26) şi echivalentele lor numerice $n_i \varepsilon \{0, 1, 2, \ldots, 25\}$, cifrul lui Cesar se poate scrie conform tabelului 1: $\mathbf{C(n_i)= n_i +3(mod26)}$

Tabelul 1 - Cifrul lui Cesar

Text clar	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Text cifrat	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Exemplu: Celebrul **"VENI VIDI VICI",** devine prin criptare : **"YHQL YLGL YLFL".**

Ulterior, cifrul lui Cesar, a fost generalizat prin alegerea în calitate de cheie a oricărei litere din alfabet.

B. Cifrul lui Polybius este un cifru substituţie. Literele alfabetului latin sunt aşezate într-un pătrat de dimensiune 5x5. Literele I si J sunt combinate pentru a forma un singur caracter, deoarece alegerea finală (între I si J) poate fi uşor decisă din contextul mesajului. Rezultă 25 de caractere aşezate într-un pătrat 5x5. Cifrarea oricărui caracter se face alegând perechea potrivită de numere (intersecţia liniei şi coloanei) corespunzătoare dispunerii caracterului în pătrat.

Pătratul lui Polybius

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Exemplu: Mesajul**: "A SOSIT TIMPUL"** se transformă după cifrare în: "11 3443344244 444223535413".

Observație: Codul poate fi schimbat prin rearanjarea literelor în pătratul 5x5.

În sistemele UNIX, programul de criptare ROT 13 este un cifru de substituție monoalfabetică; fiecare literă, în textul cifrat se rotește cu 13 caractere, de unde și denumirea de ROT 13: **C= ROT13(M),** iar decriptarea se face aplicând de două ori ROT 13, dat fiind că alfabetul latin conține N = 26 litere: **M = ROT I3(ROTI3(C)).**

Acest cifru nu este în realitate un cifru de securitate; el se utilizează adesea în posturile de utilizatori de rețea pentru a ascunde texte potențial ofensive.

Concluzie**:** Cifrurile de substituție monoalfabetică pot fi sparte cu ușurință deoarece frecvențele literelor alfabetului nu se schimbă în textul cifrat față de textul în clar.

2) *Cifruri de substituție omofonică (homophonic substitution ciphers)* sunt cifrurile de substituție în care un caracter al alfabetului mesajului în clar (alfabet primar) poate să aibă mai multe reprezentări. Ideea utilizată în aceste cifruri este uniformizarea frecvențelor de apariție a caracterelor alfabetului textului cifrat (alfabet secundar), pentru a îngreuna atacurile criptanalitice. Astfel, litera A - cu cea mai mare frecvență de apariție în alfabetul primar - poate fi înlocuită cu F, * sau K.

Concluzii:

- deși mai greu de spart decât cifrurile de substituție simple (monoalfabetice), ele nu maschează total proprietățile statistice ale mesajului în clar ;
- în cazul unui atac cu text în clar cunoscut, cifrul se sparge extrem de ușor ;
- atacul cu text cifrat este mai dificil, dar unui calculator îi va lua doar câteva secunde pentru a-l sparge.

Exemplu:

	12	14	13	0	12	14	13	0	12	14	13	0
Cuvânt cheie	M	O	N	A	M	O	N	A	M	O	N	A
Text în clar	A	S	O	S	I	T	T	I	M	P	U	L
Text cifrat	M	G	B	S	U	H	G	I	Y	D	H	L

3) *Cifruri de substituție poligramică (polygram substitution ciphers)* se obțin substituind blocuri de caractere ale alfabetului primar - numite poligrame - cu alte blocuri de caractere, de exemplu:

ABA ⟶ **RTQ**

SLL ⟶ **ABB**

Utilizări:

- Cifrul Playfair, inventat in 1854, a fost utilizat în Anglia, în timpul primului război mondial;
- Codul de compresie Huffman, bazat pe același principiu, poate fi utilizat dar este nesigur.

4) *Cifruri de substituție polialfabetice* sunt formate din mai multe cifruri de substituție simple. Au fost inventate de Leon Battista, in 1568. Dintre acestea vom aminti pe două dintre cele mai celebre și anume cele ale lui Trithemius și Vigenere.

A. Cifrul lui Trithemius este un cifru polialfabetic. Alfabetul este dispus pe 26 de linii numerotate de la 0 la 25, unde numărul de ordine al liniei indică numărul de caractere cu care se deplasează ciclic alfabetul spre dreapta. Linia numerotată cu 0 constituie tocmai alfabetul în ordinea inițială. Acest cifru poate fi utilizat astfel: primul caracter se cifrează selectându-l din linia 1, al doilea din linia a 2-a și așa mai departe.

Exemplu: 1 2 3 4 5 6 7 8 9 10 11 12

Mesajul:"A S O S I T T I M P U L" se cifrează : "B URWNZAQVZFX".

B. Cifrul lui Vigenere. Acest cifru utilizează cifrul Trithemius și un anumit cuvânt cheie. Cheia dictează alegerea liniilor în criptarea și decriptarea fiecărui caracter din mesaj.

O variantă a acestui cifru este *cifrul Vigenere cu cheie în clar (cheie de încercare)*. Cheia de încercare indică linia (sau liniile) de început pentru primul (sau primele caractere) ale textului în clar ca în exemplul următor. Apoi caracterele textului în clar sunt folosite drept chei pentru alegerea liniilor în criptare.

Exemplu: Reluăm exemplul anterior, dar alegem litera M drept cheie de încercare.

Obţinem:

Cuvânt cheie	M	A	S	O	S	I	T	T	I	M	P	U
Text în clar	A	S	O	S	I	T	T	I	M	P	U	L
Text cifrat	M	S	G	G	A	B	M	B	U	B	J	F

Observaţie: Se remarcă introducerea unei reacţii în procesul de criptare, textul cifrat fiind condiţionat de conţinutul mesajului.

O altă variantă a cifrului Vigenere este *cifrul Vigenere cu autocheie (cheie cifrată)*. După criptarea cu cheie de încercare, fiecare caracter succesiv al cheii în secvenţă se obţine de la caracterul cifrat al mesajului şi nu de la textul în clar.

Exemplu:

Cuvânt cheie	M	M	E	S	K	S	L	E	M	Y	N	H
Text în clar	A	S	O	S	I	T	T	I	M	P	U	L
Text cifrat	M	E	S	K	S	L	E	M	Y	N	H	S

Observaţie: Deşi fiecare caracter utilizat drept cheie poate fi găsit din caracterul anterior al textului cifrat, el este funcţional dependent de toate caracterele anterioare ale mesajului, inclusiv de cheia de încercare. Urmare a acestui fapt este efectul de difuziune a proprietăţilor statistice ale textului în clar asupra textului cifrat, ceea ce face ca analizele statistice să devină foarte grele pentru un criptanalist.

În baza standardelor actuale, schemele de cifrare Vigenere nu sunt foarte sigure; contribuţia importantă a lui Vigenere constă în faptul că a descoperit că pot fi generate secvenţe nerepetitive drept cheie, prin utilizarea a însuşi mesajului sau a unor părţi ale acestuia.

Cifrurile de transpoziţie se caracterizează prin faptul că textul în clar rămâne acelaşi, doar ordinea caracterelor se schimbă.

Exemplu: Cifrul simplu cu transpunere în coloane: textul în clar se scrie orizontal într-o anumită formă, ca la Polybius sau ceva asemănător, iar textul cifrat se citeşte pe verticală (coloane):

V	E	N	I
V	I	D	I
V	I	C	I

→ ''V V E I I N D C I I I''

O simplă transpoziţie permite păstrarea proprietăţilor statistice ale textului în clar şi textului cifrat; o nouă transpoziţie a textului cifrat măreşte securitatea cifrului.

Utilizări: ADFGVX, utilizat de germani în timpul primului război mondial are un cifru substituţie combinat cu o altă substituţie; deşi pentru acea vreme a fost foarte complex, el a fost spart de criptanalistul francez Georges Painvin.

Mulţi algoritmi moderni folosesc transpoziţia, dar consumul de memorie este mare comparativ cu substituţia, care din acest punct de vedere este mai convenabilă.

Maşini rotor

În vederea mecanizării complicatelor metode de substituţie si permutărilor repetate, în anul 1920 au fost inventate o serie de echipamente mecanice de criptare bazate pe principiul de rotor. *0 maşină rotor (rotor machine)* are o tastatură şi o serie de rotoare ce permit implementarea unei versiuni a cifrului Vigenere. Fiecare rotor face o permutare arbitrară a alfabetului, are 26 de poziţii şi realizează o simplă substituţie. Deoarece rotoarele se mişcă cu viteze de rotaţie diferite, perioada unei maşini cu n rotoare este 26^n.

Cel mai celebru cifru bazat pe o maşină rotor este Enigma, utilizată de germani în cel de-al doilea război mondial. El a fost inventat de Arthur Scherbius şi Arvid Gerhard Damm în Europa şi a fost patentată în SUA. Germanii au îmbunătăţit considerabil proiectul inventatorilor săi, dar a fost spart de criptanaliştii polonezi care au explicat atacul lor englezilor.

Bibliografie

1) Angheloiu, I., Gyorfi, E., Patriciu, V.V. (1986): *Securitatea şi protecţia informaţiei în sistemele electronice de calcul,* Ed. Militară, Bucureşti

2) Angheloiu, I.(1972): *Teoria codurilor,* Ed. Militară, Bucureşti

3) Borda, M. (1999): *Teoria transmiterii informaţiei,* Dacia, Cluj-Napoca

4) Deavours, C.A., Kahn, D. (1998): *Selections from Cryptologia,* Artech House

5) Hankerson, D. R., Hoffman, D. G., Leonard, D. A., Lînder, C.(2000): *Coding Theory and Cryptographv: The Essentials (Pure and Applied Mathematics,* Vol 234), Marcel Dekker, Rev&ex, 2nd edition, Sep.

6) India International Conference in Cryptology in India 2000 Calcutta (2000): *Progress in Cryptology,* Indocrypt 2000 Proceedings of the First International Conference in Cryptology Calcutta, Springer Verlag, Dec.

7) McCurley, K. S., Ziegler, C. D. (1999): *Advances in Cryptology,* 1981-1997 Electronic Proceedings and index of the Crypto and Eurocrypt Conferences 1981 -1997 (Lecture Notes in Computer Science), Springer Verlag, Jun.

8) Patriciu V.V. (1998): *Securitatea informatică în UNIX si Internet,* Ed. Tehnică, Bucureşti

9) Patriciu, V.V. (1994): *Criptografia şi securitatea reţelelor de calculatoare,* Ed. Tehnică, Bucureşti

10) Stallings, W. (1999): *Cryptography and Network Security — Principles and Practice,* Prentice Hall, Second Edition

11) T.I.Băjenescu, M.E.Borda – *Securitatea în informatică şi telecomunicaţii*; Ed. Dacia, Cluj Napoca, 2001

12) V.V. Patriciu, M.Ene-Pietroşanu – *Securitatea Comerţului Electronic* – Ed. All, Bucureşti, 2001

13) V.V.Patriciu, M.Ene-Pietroşanu – *Securitatea în Informatică în UNIX şi Internet* – Ed. Tehnică, Bucureşti, 1998