Tehnici de CRIPTARE

Claudiu Soroiu

Criptarea mesajelor este unul dintre cele mai studiate domenii din zilele noastre. Complexitatea tehnicilor de criptare și de trimitere a mesajelor crește permanent pentru a obține o securitate cât mai ridicată a comunicațiilor. Pe parcursul câtorva episoade, vom prezenta unele dintre cele mai cunoscute modalități de codificare a mesajelor.

Introducere

Criptarea mesajelor și trimiterea lor sub această formă este utilizată de foarte mult timp. Unul dintre primii care au folosit tehnici de criptare pentru trimiterea mesajelor a fost celebrul împărat roman *Cezar*. În comunicarea privată cu o persoană, folosirea unui cod secret poate preveni citirea intenționată sau neintenționată a mesajelor de către cei care intră în posesia acestora, fie pentru că trebuie să le transporte până la destinatar, fie pentru că le interceptează în timp ce mesajul este transmis.

Definiție

Criptarea reprezintă o metodă prin care un *text necriptat* (documente, fișiere, fraze, cuvinte etc.) este transformat, utilizând anumite metode, într-un alt text, numit ***text criptat***, care se păstrează în această formă sau se trimite unei anumite persoane. Criptarea este utilizată cu scopul de a păstra secretul unei anumite informații. În cazul în care informația criptată ajunge și la alte persoane, altele decât cele care trebuie să o primească sau să o păstreze, nu se poate obține textul original decât dacă este cunoscută tehnica de criptare folosită și, eventual, o parolă utilizată în procesul de criptare.

Procedeul invers prin care un text criptat este transformat în textul original poartă numele de ***decriptare***.

Există foarte multe tehnici de criptare cunoscute de foarte multe persoane, dar cu toate acestea, pentru tehnicile avansate, datorită complexității algoritmilor folosiți pentru codificare, procesul invers, cel de *decriptare*, este aproape imposibil de realizat.

Un algoritm de criptare este cu atât mai eficient, cu cât textul criptat și eventuala parolă utilizată sunt foarte greu de găsit, chiar dacă cel care încearcă să decripteze textul deține o parte din textul inițial. Un alt factor important de care depinde eficiența unui algoritm de criptare implementat într-un anumit limbaj de programare este timpul folosit de programul respectiv pentru a codifica o cantitate foarte mare de informații. Un text criptat folosind o metodă care nu necesită cunoștințe vaste din domeniul matematicii și informaticii este foarte ușor de decriptat.

Criptarea lui Cezar

Când trimitea mesaje oficiale către subalternii săi, *Cezar* folosea o tehnică foarte simplă de codificare a acestora. Fie două cercuri pe care sunt scrise cele 26 de litere ale alfabetului englezesc; dacă rotim cercul mic cu un număr de litere față de celălalt în sensul acelor de ceasornic, atunci, pentru a cripta un mesaj, se caută fiecare literă din mesaj pe cercul mare și se scrie litera corespunzătoare de pe cercul mic.

Figura 1

Figura 2

Dacă avem textul *IULIUS CAESAR* și deplasăm cercul din interior din figura 1 cu două litere în sensul acelor de ceasornic după cum se observă în figura 2, atunci textul criptat va fi *GSJGSQ AYCQYP*.

Procedeul de rotire a cercului mic cu un anumit număr de litere poartă numele de ***deplasare***. Pentru această tehnică de criptare, o parte din cheia (***parola***) de criptare o constituie numărul de deplasări (***deplasament***) de câte o literă în sensul acelor de ceasornic. Cealaltă parte din cheia de

criptare o constituie alfabetul ales. Alfabetul folosit poate să fie altul decât cel prezentat în exemplul anterior. Acesta poate să conțină pe lângă majuscule și alte caractere printre care pot apărea cifre, caractere speciale, alte litere ale alfabetelor diferitelor limbaje utilizate sau poate să fie întreg setul de caractere ***ASCII*** folosit de calculator.

Pentru a decripta un mesaj criptat cu această metodă, trebuie să se cunoască numărul de deplasări utilizat la criptarea textului inițial. Procesul de obținere a mesajului inițial din mesajul criptat când se cunoaște deplasamentul este foarte simplu. Se deplasează cercul din interior cu atâtea litere cu câte indică deplasamentul și fiecare literă din textul criptat se caută pe cercul din interior și se scrie litera corespunzătoare de pe cercul din exterior. Din textul *FRIFRP ZXBPXO* criptat în cazul alfabetului englezesc, folosind un deplasament de trei caracactere, prin decriptare se obține *IULIUS CAESAR*.

Dacă notăm cu *L* numărul de caractere al alfabetului utilizat, atunci textul criptat folosind un deplasament *D* mai mare sau egal cu *L* este același cu cazul în care deplasamentul este restul împărțirii lui *D* la *L*.

Această metodă de criptare nu este eficientă, deoarece textul criptat poate fi ușor decriptat dacă se cunoaște alfabetul utilizat. La decriptare se folosesc *L* deplasamente și astfel se generează *L* texte dintre care numai unul este cel bun și poate fi ușor identificat.

Variante ale criptării lui Cezar

O variantă a criptării lui *Cezar* este tehnica folosită de *Ovidius.* Acesta nu folosea deplasarea cercului din interior, în schimb literele de pe cercul din interior erau scrise în ordine inversă (de la ultima literă din alfabet la prima, în sensul acelor de ceasornic). Acest lucru este echivalent cu scrierea literelor din alfabet pe un rând în ordine și pe celălalt rând în ordine inversă, după cum se poate observa în continuare:

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

Pentru a cripta cuvântul *OVIDIUS* se caută pentru fiecare literă din cuvânt litera de pe primul rând și se scrie litera de pe al doilea rând de sub litera găsită. Aplicând acest procedeu obținem cuvântul *MERWRFH*.

Pentru decriptare se folosește același procedeu ca în cazul criptării deoarece, dacă unei litere *i* de pe primul rând îi corespunde a (*L* + 1 - *i*)-a literă din al doilea rând, atunci celei de-a (*L* + 1 - *i*)-a litere din primul rând îi corespunde a (L + 1 -(*L* + 1 - *i*))-a literă din al doilea rând, adică a *i*-a literă.

Criptarea cu alfabet aleator

O altă variantă a criptării lui *Cezar* este folosirea unui alfabet și aranjarea caracterelor acestuia, pe cele două cercuri, într-o ordine aleatoare, dar caracterele de pe ambele cercuri trebuie să fie aranjate în aceeași ordine.

Pentru decriptarea mesajelor criptate cu ajutorul unui alfabet ales aleator, trebuie cunoscute alfabetul, ordinea caracterelor din alfabet precum și numărul de deplasări. Având aceste componente, procesul de decriptare este similar celui prezentat în secțiunea anterioară.

Dacă se folosește alfabetul englezesc, ca posibilă modalitate de aranjare a caracterelor pe cele două cercuri ar putea fi aleasă aranjarea lor de pe tastatură, și anume:

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

În cazul în care se cunoaște numai tehnica de criptare utilizată, decriptarea mesajului este mai complicată, deoarece se bazează pe statistică matematică și în principal pe faptul că într-un text necriptat cu o dimensiune suficient de mare vocalele au o frecvență foarte mare și nu există două vocale consecutive din text care să fie la o distanță mai mare de șase caractere (pentru limba română).

Metoda substituției

Prin *substituție* se înțelege înlocuirea fiecărui caracter din alfabet cu un altul și nu există două caractere care să fie înlocuite cu același caracter. O altă posibilitate ar fi aceea de a înlocui fiecare caracter din alfabetul ales cu un simbol sau un număr.

Tehnicile de criptare prezentate până acum sunt cazuri particulare ale criptării prin substituție.

Considerând alfabetul englezesc, există 26! posibilități de substituire a caracterelor cu altele din care, pentru o mai mare securitate a datelor se scade numărul de posibilități în care un caracter este substituit cu el însuși (acest număr se obține rezolvând *problema concordanțelor*).

Criptarea unui text folosind această metodă se face ca în cazul criptării lui *Ovidius*, adică pentru fiecare caracter din text se scrie litera care s-a ales pentru substituție.

Fie următoarea aranjare a caracterelor alfabetului englezesc:

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

Pentru textul *PAROLA ESTE ASDFG*, mesajul criptat folosind aranjarea de mai sus, este: *NZFEDZ JOXJ ZOASB*.

Procesul de decriptare se face în sens invers, adică pentru fiecare literă din textul criptat se scrie litera pe care aceasta a substituit-o în procesul de criptare.

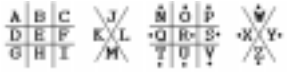
Caracterele se pot substitui și cu numere, existând mai multe variante a acestui procedeu. De exemplu, fiecărui caracter i se poate asocia o mulțime de numere care îl pot substitui, dar mulțimile asociate caracterelor alfabetului ales trebuie să fie disjuncte. Dacă pentru litera **A** se alege o mulțime $\{n_1, n_2, ..., n_m\}$, oricare din elementele mulțimii pot substitui această literă. În procesul de criptare, pentru fiecare literă din textul inițial se alege aleator un număr din mulțimea care i-a fost atribuită.

De exemplu, dacă pentru caracterul **A** se alege mulțimea {1, ..., 10}, pentru litera **B** se alege mulțimea {11, ..., 20} etc., există mai multe posibilități pentru a cripta textul de mai sus; una dintre ele poate fi: 154, 7, 172, 149, 120, 156, 48, 185, 194, 44, 4, 184, 33, 51, 63.

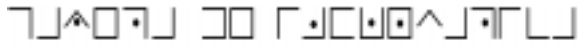
Nu este obligatoriu ca mulțimile alese pentru fiecare caracter să aibă același cardinal; de fapt, este indicat ca

mulțimile asociate literelor care apar frecvent să aibă mai multe elemente.

Pentru transmiterea de texte criptate se mai pot folosi imagini în care caracterele din textul inițial sunt înlocuite cu simboluri predefinite. Una dintre cele mai cunoscute metode de înlocuire a caracterelor cu simboluri este prezentată în figura următoare.



Pentru fiecare caracter din figură se desenează conturul regiunii în care acesta se află. De exemplu, pentru litera N se desenează laturile regiunii din stânga-sus ale diagramei în care se află împreună cu un punct între laturi. Folosind aceste simboluri, textul *GAZETA DE INFORMATICA* se scrie astfel:



Metoda transpoziției

Criptarea prin *metoda transpoziției* este o tehnică mai eficientă decât criptarea prin substituție, dar are, la rândul ei, o mulțime de dezavantaje.

Textul criptat prin metoda transpoziției păstrează toate caracterele textului inițial, dar în altă ordine obținută prin aplicarea algoritmului ce va fi prezentat în continuare.

Criptarea prin transpoziție constă din scrierea textului inițial din care s-au eliminat spațiile și semnele de punctuație, într-o matrice de dimensiune $M \times N$, interschimbarea anumitor linii (sau coloane) între ele și textul criptat se obține prin scrierea caracterelor din noua matrice de pe fiecare coloană în parte, începând cu colțul din stânga-sus. Dacă lungimea textului inițial este mai mică decât numărul de elemente ce pot fi scrise în matrice, atunci textul se completează cu elemente aleatoare, până ajunge la dimensiunea $M*N$.

Pentru textul *Misiunea a fost îndeplinită*, care are lungimea de 24 de caractere, se pot alege mai multe matrice de dimensiune $M \times N$, o posibilitate ar fi ca matricea să aibă 4 linii și 6 coloane, dar pentru ca textul să fie mai greu de decodificat trebuie să conțină și caractere alese aleator, sau într-un mod mai inteligent, care să îngreuneze munca celui care dorește să afle conținutul secret din mesajul criptat. Fie o matrice care are 5 linii și 6 coloane. Textului inițial i se adaugă 6 caractere aleatoare și se obține textul *Misiu neaaf ostîn depli nităx yztwu* și se scrie în matricea din partea stângă astfel:

	1	2	3	4	5	6
1	M	i	s	i	u	n
2	e	a	a	f	o	s
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
5	x	y	z	t	w	u

	1	2	3	4	5	6
5	x	y	z	t	w	u
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
1	M	i	s	i	u	n
2	e	a	a	f	o	s

Prin scrierea liniilor 1, 2, 3, 4, 5 în ordinea 5, 3, 4, 1, 2, se obține matricea din partea dreaptă. Textul criptat care se obține este: *xtlMe yîiia znnsa tdiif wetuo upăns*.

Transpoziție cu parolă

Pentru ca procesul de decriptare să fie mai simplu și să nu mai fie nevoie ca ordinea în care au fost puse liniile din matricea creată, se folosește o variantă a criptării prin transpoziție care se bazează pe o parolă.

Pentru a cripta un text folosind o parolă și metoda transpoziției, se alege o parolă ale cărei litere determină ordinea în care se vor scrie coloanele din matricea aleasă.

Pentru a afla ordinea în care vor fi scrise coloanele din textul inițial, se ordonează alfabetic literele din parolă, și fiecărei litere i se asociază numărul de ordine din șirul ordonat.

Lungimea parolei trebuie să fie egală cu numărul de coloane din matrice.

Considerăm textul anterior, scris într-o matrice de dimensiuni 5×6, și parola *vultur*. Literele din parolă se ordonează alfabetic și se obține șirul: *l*, *r*, *t*, *u*, *u*, *v*. Indicele 1 este asociat cu litera *l*, indicele 2 cu litera *r*, indicele 3 cu litera *t*, indicele 4 cu prima literă *u* din parolă, indicele 5 cu a doua literă *u* din parolă, iar indicele 6 este asociat cu litera *v*. Pentru a scrie coloanele, pentru fiecare indice *i* din șirul ordonat se caută indicele *j*, care reprezintă poziția literei cu indicele *i*, din parolă și se scrie coloana *j*, astfel:

	v	u	l	t	u	r
	6	4	1	3	5	2
1	M	i	s	i	u	n
2	e	a	a	f	o	s
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
5	x	y	z	t	w	u

	1	2	3	4	5	6
5	s	n	i	i	u	M
3	a	s	f	a	o	e
4	n	p	d	î	e	t
1	n	ă	i	i	t	l
2	z	u	t	y	w	x

Textul care se obține în final este: *sannz nspău ifdit iaîiy uoetw Metlx*.

Pentru a decripta un mesaj criptat folosind această metodă, mesajul se scrie în matrice pe coloane, începând cu colțul stânga-sus, și apoi se realizează operația inversă, adică pentru fiecare indice *j* al literelor din parolă, se caută indicele *i* asociat literei din șirul sortat și se scrie coloana cu indicele *i*. Din noua matrice astfel obținută se scriu literele de pe fiecare linie, în ordine.

O tehnică foarte cunoscută și foarte practică de transmitere a mesajelor folosind metoda transpoziției constă în înfășurarea unei panglici în jurul unui băț. Mesajul se scrie pe panglică, de-a lungul bățului, de la capătul superior spre capătul inferior, pe coloane și apoi se trimite la destinație numai panglica, care ulterior s-a desfăcut de pe băț. La destinație se înfășoară panglica pe un băț având aceeași dimensiune cu cel care a ajutat la scrierea textului și se citește textul pe coloane.

Această tehnică de transmitere a mesajelor criptate era folosită chiar și în antichitate.

De atunci anii au trecut și tehnicile de criptare au evoluat foarte mult. În numărul următor vom prezenta câteva dintre tehnicile avansate de criptare avansate.

Claudiu Soroiu este redactor al GInfo. Poate fi contactat prin e-mail la adresa csoroiu@yahoo.com.