

CRİPTOGRAFIA

Arta păstrării secretelor

JOAN VICENÇ GÓMEZ I URGELLÉS

Traducere de Luiza Stroe

CUPRINS

Capitolul 0

R de la Rivest, S de la Shamir și A de la Adleman: despre algoritmi și securitate cibernetică

49 6e 74 72 6f 64 75 63 63 69 f3 6e	7
<i>Criptografia muzicală</i>	12
<i>Kryptos: un secret la ușa CIA</i>	16
<i>Câte chei sunt necesare?</i>	17
Numerele prime: gazdele familiei și complici ai sistemelor de securitate	18
<i>Câteva sfaturi pentru uz casnic</i>	21

Capitolul 1

Secretele de-a lungul istoriei

<i>Kamasutra</i>	23
Regina martiră: codurile secrete ale conspirației Babington	25
De la Sparta la Războiul Galic. Criptare elementară: transpoziție și substituție	27
Criptare de înlocuire: criptarea lui Polybius și codul Cezar	29
Matematica secretelor	33
Suma și produsul în $\mathbb{Z}/(n)$	36
<i>Algoritmul lui Euclid și cel mai mare divizor comun</i>	40
Ucenic hacker	42
<i>Cifrul afin</i>	45
Analiză de frecvență	46
<i>Criptografi în literatură: Edgar Allan Poe și Jules Verne</i>	48
Coduri de bare	49
ISBN: cartea de identitate a cărților	52
O plimbare prin bancă	55
<i>Cifrul Hill</i>	62

Capitolul 2

Criptări polialfabetice	65
Alberti, Gronsfeld și Vigenère	65
Cifrul lui Verman, telefonul roșu și Revoluția Cubaneză	77
Două cifruri clasice: Playfair și ADFGVX	80
Ținta Paris: cifrul ADFGVX	82
Turing, Von Neuman și Enigma	87
<i>Codul Morse</i>	88
<i>Turing, Clarke și Neumann</i>	91

Capitolul 3

Societatea zerourilor și a unu-urilor: protagoniști ai unui nou limbaj	93
Codul ASCII, limbajul calculatoarelor	93
<i>Sistemul de numerotare zecimală și echivalența în binar</i>	94
Vernam și operatorul XOR	96
<i>Cartea de identitate a calculatoarelor: adresa IP</i>	98
Sistemul hexazecimal	100
Rețele fără fir	103
<i>Trecerea de la sistemul de numerotare hexazecimală la sistemul zecimal</i>	103
Transmiterea informațiilor: Shannon și Hamming	106
<i>Claude Elwood Shannon</i>	107
<i>Richard W. Hamming</i>	111
Secrete în epoca moduloernă	112
<i>Diffie-Hellman</i>	116
<i>Premiul Turing</i>	119
Sistemul cheii publice RSA	120
<i>Algoritmul RSA</i>	123
ElGamal	126
Funcții Hash	128
<i>Funcția hash și norme de trafic</i>	131
Semnătura digitală	132
Curbe eliptice	137
Bibliografie recomandată	143

Capitolul 0

R de la Rivest, S de la Shamir
și A de la Adleman: despre algoritmi
și securitate cibernetică

49 6e 74 72 6f 64 75 63 63 69 f3 6e

Cu siguranță, cititorul va fi oarecum surprins de titlul acestei secțiuni, care este, nici mai mult, nici mai puțin, cuvântul *introducere* în așa-numitul „cod hexazecimal”, care la rândul său este tradus în binar ca:

01001001 01101110 01110100 01110010 01101111 01100100
01110101 01100011 01100011 01101001 11000011 10110011
01101110 00001101 00001010

Astăzi, această transpunere este un proces simplu. Cititorul poate transpune în diferite limbaje (în special, de la binar la hexazecimal și invers) pe site-ul web: <https://goo.gl/SmF28U>. În această carte vor fi prezentate aceste limbaje și rolul lor genial în transmiterea secretelor, deoarece lumea codurilor și a securității este familiarizată cu această tipologie de limbaj. Îi vom descoperi sensul, evoluția și interpretarea și, pe măsură ce lectura avansează, se vor putea găsi răspunsuri la întrebări neobișnuite de tipul: care este relația dintre împăratul Iulius Cezar, Euclid, *Kamasutra* și actul nostru de identitate? Și care dintre internet, Leonhard Euler și numerele prime?

Când apare o pictogramă de lacăt pe calculatorul nostru și scriem o parolă, ceea ce se activează, în majoritatea cazurilor, este protocolul RSA: două calculatoare comunică printr-un algoritm matematic. RSA este cel mai popular dintre așa-numitele sisteme criptografice cu cheie publică. Dezvoltat în 1977 de **Ronald Linn Rivest** (n. 1947), **Adi Shamir** (n. 1952) și **Leonard Adleman** (n. 1945), de la Massachusetts Institute of Technology (MIT), este cel mai utilizat algoritm atât pentru criptare, cât și pentru semnarea digitală. După cum vom vedea, este un protocol bazat pe factorizarea numerelor întregi în numere prime. Ca în orice sistem criptografic cu cheie publică, fiecare utilizator are două chei de criptare: una publică și cealaltă numită privată. Când doriți să trimiteți un mesaj, expeditorul folosește cheia publică a destinatarului pentru a-și cripta mesajul, iar destinatarul, atunci când îl primește, se ocupă de decriptarea acestuia folosind cheia sa privată. În sistemul RSA, mesajele trimise sunt reprezentate prin numere, iar funcționarea se bazează pe produsul cunoscut a două numere prime mari alese la întâmplare și ținute secrete.

Poate părea complex – și este –, dar RSA poate fi explicată sub forma unei „ghicitori”: care două numere trebuie înmulțite pentru ca rezultatul să fie 15? Este simplu: 3×5 . Acum imaginați-vă că numărul este 58 732 567. Descompunerea acestuia este mai complicată, dar un calculator o face cu ușurință. De fapt, rezultatul ar fi: $58\,732\,567 = 1721 \cdot 34\,127$. Acum, dacă numărul total este format din 200 de cifre și, în plus, este rezultatul înmulțirii a două numere prime, este greu de aflat care două numere au fost înmulțite pentru a-l crea. Însă crearea acestuia este relativ ușoară. Aceasta este ingeniozitatea invenției.

Când Rivest și colegii săi au provocat comunitatea matematică, la sfârșitul anilor 1970, cu problema lor RSA, au crezut că nimeni nu o poate rezolva în 40 de miliarde de ani. Erau puține calculatoare și web-ul nu exista. Sistemul RSA a apărut pentru prima dată în august 1977. În revista *Scientific American*, Martin Gardner (1952–2000) a scris în secțiunea de hobby de matematică articolul „Un nou tip de

număr a cărui descifrare ar dura milioane de ani”, în care a provocat cititorii. Articolul prezintă un text criptat a cărui cheie pentru codificare a constat în factorizarea numărului n :

$$n = 114\ 381\ 625\ 757\ 888\ 867\ 669\ 235\ 779\ 976\ 146\ 612\ 010\ 218\ 296$$

$$721\ 242\ 362\ 562\ 561\ 842\ 935\ 706\ 935\ 706\ 935\ 245\ 733\ 897\ 830\ 597$$

$$123\ 563\ 958\ 705\ 058\ 989\ 075\ 147\ 599\ 290\ 026\ 879\ 543\ 541$$

ca produs al două numere prime p și q , care se foloseau pentru decodificare. Premiul a fost de 100 de dolari, o sumă foarte atrăgătoare în 1977, iar cititorii au fost încurajați să-și trimită răspunsul la laboratorul de calculatoare MIT. Arhitecții sistemului RSA, Rivest, Shamir și Adleman, au primit peste trei mii de răspunsuri, iar cel care a fost primit la 26 aprilie 1994 (șaptesprezece ani mai târziu) cu colaborarea a peste 600 de oameni, a fost următorul: $n = p \cdot q$, astfel încât

$$p = 32\ 769\ 132\ 993\ 266\ 709\ 549\ 961\ 988\ 190\ 834\ 461\ 413\ 177\ 642$$

$$967\ 992\ 942\ 539\ 798\ 288\ 533\ \text{și}$$

$$q = 3\ 490\ 529\ 510\ 847\ 650\ 949\ 147\ 849\ 619\ 903\ 898\ 133\ 417\ 764$$

$$638\ 493\ 387\ 843\ 990\ 820\ 577.$$

Mesajul era: *the magic words are squeamish ossifrage* (cuvintele magice sunt un vultur bărbos impresionant). În prezent, mesaje de peste 300 de cifre pot fi rezolvate cu acest sistem, deși chiar și celor mai puternice calculatoare le este greu să factorizeze cifre de asemenea amploare. Dacă nu se va găsi un algoritm care să factorizeze numerele de acest tip, putem garanta că sistemul RSA este până acum una dintre metodele cele mai sigure de criptare și una dintre cele mai faimoase așa-numite „chei publice”. Anual are loc un Congres exclusiv RSA; informații despre acesta pot fi obținute la [https:// www.rsaconference.com](https://www.rsaconference.com).

Tranzacțiile comerciale pe internet depind de numere prime, ceea ce le conferă o valoare deosebită pentru afaceri, comunicații, semnături electronice, registre etc. Cunoașterea modului în care sunt distribuite și, astfel, posibilitatea de a obține numere prime din ce în ce mai mari, care servesc drept cheie criptografică, este o mare provocare pentru tehnologii și pentru matematică în sine.

Dar înainte de a trece mai departe în aceste subiecte, poate că merită să privim mai întâi în urmă și să înțelegem, în linii mari, cei mai relevanți pași din istoria criptografiei.

§

Criptografia este arta de a scrie cu o cheie secretă sau într-un mod enigmatic. Provine din grecescul *kryptos*, „ascuns”, și *graphein*, „a scrie”, iar ca disciplină este responsabilă de studiul codurilor secrete legate de securitate în schimbul de mesaje codificate între un expeditor și un destinatar.

În lumea criptografiei, termenii *cod* (sau *criptare*) și *codare* (sau *codificare*) sunt obișnuite. Codarea înseamnă schimbarea unui text în „altceva” (simboluri, alfabete, numere etc.) de comun acord. În timp ce *criptarea* se referă la algoritmi matematici care sunt prezenți în acea traducere.

Esența securității în transmiterea informațiilor (verbală, scrisă, telematică etc.) datează din Antichitate și a supraviețuit până în zilele noastre. Este, nici mai mult, nici mai puțin, decât teama că „cineva” din afara noastră va „descoperi” secretele noastre cele mai adânci, ceea ce compromite în mod clar intimitatea și securitatea. În 1948, matematicianul și criptograful american **Claude E. Shannon** (1916–2001) a definit secretul perfect drept „un sistem care rezistă oricărui atac, chiar și cu putere de calcul și timp infinite. Diagrama din figura 1 ilustrează un canal de comunicare „secret”.

Obiectivul criptografiei nu este de a ascunde existența unui mesaj, ci mai degrabă de a ascunde sensul acestuia de cei care nu ar trebui

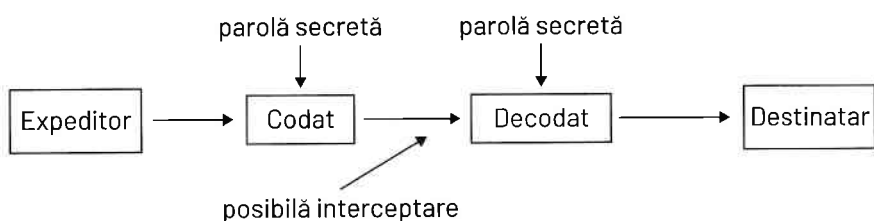


Figura 1.

să-l cunoască. În acest scop, se folosește „codarea”. Rolul matematicii nu este prezent doar în criptografie, ci și în procesul de decriptare a mesajelor criptate, care este cunoscut sub numele de „criptanaliză”.

Civilizațiile antice dezvoltaseră deja tehnici de transmitere a mesajelor în timpul conflictelor militare, astfel încât dacă mesagerul ar fi fost interceptat, informațiile să nu cadă în mâinile inamicului. Una dintre cele mai vechi metode datează din secolul al V-lea î.Hr., *Scitalul*. Îl vom analiza în detaliu în capitolul 1, dar menționăm aici că acest sistem de transpunere, constând în alterarea ordinii elementelor unui mesaj, a fost folosit de eforii spartani. Era format din două tije identice, cu același număr de fețe. O tijă trebuia să fie în mâinile expeditorului mesajului; cealaltă, în cele ale destinatarului. Pe acea tijă se înfășura o bandă în spirală și se scria un mesaj pe lungimea sa. Odată ce mesajul era terminat, banda era trimisă destinatarului. Acesta, înfășurându-o pe tija lui, îl putea descifra.

Figura 2. Scitalul.



CRİPTOGRAFIA MUZICALĂ

Metoda de ascundere a mesajelor în partituri și melodii muzicale este cunoscută sub denumirea de „criptografie muzicală”. Militarul și scriitorul englez Philip Thicknesse (1719–1792) a publicat în 1772 *A Treatise on the Art of Deciphering, and of Writing in Cypher: With an Harmonic Alphabet*, unde a propus utilizarea așa-numitului „alfabet armonic”, care constă în asocierea anumitor sunete și note muzicale cu litere ale alfabetului, în așa fel încât notele care fac parte dintr-un cântec configurează la rândul lor mesajul ascuns.

Se știe că faimosul spion olandez Mata Hari (1876–1917) a folosit această criptare pentru a trimite mesaje secrete aliaților săi. De aceea, această formă de criptare este adesea numită și „criptare Mata Hari”, și constă în înlocuirea notelor scalei muzicale cu literele alfabetului: începând cu nota *La*, care ar fi A; *Si bemol* ar fi B; *Do* ar fi C, iar *Fa* ar fi D. Prin această metodă, mai mulți compozitori și-au înregistrat propriile nume în lucrările pe care le-au compus, de exemplu, Johann Sebastian Bach (1685–1750), care, urmând nomenclatura tradițională germană, corespunde cu:

B	A	C	H
SI	LA	DO	SI

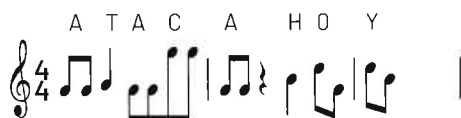
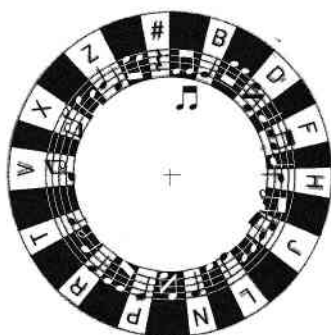
În acest fel, compunând acea melodie, obținem numele autorului. Alți compozitori au folosit același cod, cum ar fi Francis Poulenc (1899–1963)

Mai târziu, românii au schimbat sistemul de transpunere în cel al substituirii caracterelor, dintre care cel mai mediativ este cunoscut sub numele de *codul lui Cezar* (vezi figura 3), deoarece se presupune că Iulius Cezar (100–44 î.Hr.) l-a folosit în campaniile sale de război.

în *Valsul improvizat pe numele lui Bach*. În general, această criptare corespunde unei simple criptări de înlocuire, care este una dintre cele mai simple existente.

Ideea de criptare muzicală a fost considerată o tehnică imbatabilă, deoarece se credea că o partitură a unei melodii fără versuri nu ar provoca suspiciuni. Criptografia muzicală nu a fost foarte mediatizată, deoarece nu se cunosc transmisii de mesaje relevante în lumea spionajului cu acest sistem, poate din cauza mediului ales în care mesajul trebuie ascuns. Cu toate acestea, de-a lungul istoriei nu lipsesc exemplele de utilizare a acestuia.

Figura 3. Cu această roată simplă am putea transmite mesaje tactice sub formă de șuruburi, de exemplu.



În 1465, arhitectul italian **Leon Battista Alberti** (1404–1472) a inventat un nou sistem de codare care face parte din algoritmi cunoscuți sub numele de „substituție polialfabetică” și a adus mari progrese în arta ascunderii secretelor. Un alt criptograf important, din

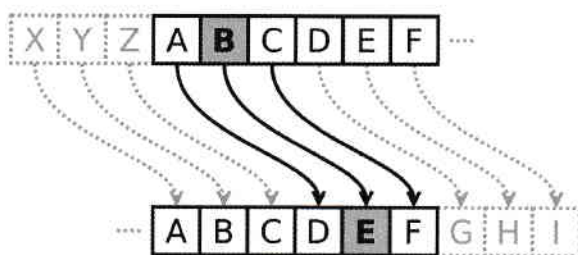


Figura 4. Sistemul de criptare Cezar. Este una dintre cele mai simple și mai utilizate tehnici de criptare. Conform acestui sistem, o literă în textul original este înlocuită cu alta care se regăsește la un număr fix de poziții decalate în alfabet.

secolul al XVI-lea, a fost francezul **Blaise de Vigenère** (1523–1596), autor al unui important tratat despre „scrierea secretă”, intitulat *Traicté des Chiffres*, care a conceput un cifru cunoscut până în zilele noastre și asociat cu numele lui. Din secolul al XVI-lea datează și povestea Mariei Stuart (1542–1567), regina Scoției, care a fost executată de verișoara ei Elisabeta I, regina Angliei, când complotul i-a fost descoperit datorită unei criptoanalize reușite de către colaboratorii Elisabetei.

Timp de mai multe secole, interesul monarhilor pentru criptografie a fost remarcabil. Trupele regelui spaniol Filip al II-lea (1527–1598) au folosit frecvent un sistem de codare cu un alfabet de peste 500 de simboluri pe care matematicienii regelui îl considerau inexpugnabil. În asemenea grad încât, atunci când matematicianul francez **François Viète** (1540–1603) a reușit să descifreze acest sistem pentru Regele Franței, curtea spaniolă a depus o plângere la Papa Pius al V-lea în care îl acuza pe monarhul Henric al IV-lea că folosește magie neagră.

În secolul al XIX-lea se remarcă figura ofițerului de infanterie, criptograf și arheolog prusac **Friedrich Wilhelm Kasiski** (1805–1881), care a conceput o metodă criptografică bazată pe căutarea cuvintelor repetate. Analiza repetărilor a făcut posibilă cunoașterea lungimii

cheii utilizate în criptare. În timpul Primului Război Mondial, germanii au folosit așa-numitul „cifru ADFGVX”, similar altor metode de substituție aplicate în Grecia Antică. Era format dintr-o matrice 6×6 folosită pentru a înlocui orice literă a alfabetului și numerele de la 0 la 9 cu o pereche de litere care combinau: A, D, F, G, V sau X. Astfel, VV-ul va fi descifrat ca R conform următorului tabel al acestui sistem:

	A	D	F	G	V	X
A	3	p	6	d	l	1
D	l	t	4	o	a	h
F	7	K	b	C	5	Z
G	J	U	G	W	G	M
V	X	S	V	I	R	2
X	9	e	y	O	f	q

La mijlocul secolului XX, și mai ales în timpul celui de-al Doilea Război Mondial, criptografia a început să folosească un nou instrument care să facă posibilă realizarea unei criptări mai bune și mai sigure, din momentul în care au apărut mașinile numerice, printre care mașina germană Enigma. Enigma este o mașină cu rotor care a automatizat foarte mult calculele necesare pentru operațiunile de criptare și decriptare a mesajelor. Pentru a învinge ingeniozitatea germană și pentru a crea mașini precum Enigma, a fost necesară implicarea celor mai buni matematicieni ai vremii, inclusiv **Alan Turing** (1912–1954), și un mare efort de calcul. Deloc surprinzător, cele mai mari progrese atât în domeniul criptografiei, cât și al criptoanalizei au avut loc în acel moment.

KRYPTOS: UN SECRET LA UȘA CIA

Kryptos, construită în 1990 de sculptorul James Sanborn (n. 1945) în curtea campusului Langley (Virginia), la intrarea în sediul CIA, este numele sculpturii care ascunde un mesaj pe care nimeni nu l-a putut rezolva.

Să ne amintim că *kryptos* înseamnă „ascuns”. *Kryptos* ascunde patru mesaje criptate ($k1$, $k2$, $k3$, $k4$) în limba engleză, împărțite pe 865 de caractere. Recent, David Stein, un analist CIA, și Jim Gillogly, un informatician din California, au spart trei sferturi din criptare. Totuși, $k4$, alcătuit din 97 sau 98 de caractere (în funcție de faptul că semnul întrebării este inclus sau nu în textul dintre această secțiune și cea anterioară), nu a fost încă descifrat; În acest sens, James Sanborn însuși a oferit indicii: primul este cuvântul Berlin, al doilea, ceas. Mesajul descifrat astăzi spune: „Între umbrirea subtilă și absența luminii se află nuanța iluziei”.

Tocmai în acest punct se poate observa nașterea criptografiei moderne, în care se remarcă matematicianul menționat mai sus, Claude E. Shannon, și contribuția sa la cercetarea în teoria informației. În plus, dezvoltarea calculului automat a reprezentat și o oportunitate pentru avansarea noilor sisteme. În cele din urmă, la începutul anilor 1970, intră în scenă trei personaje care sunt pionierii algoritmilor actuali de codare: Rivest, Shamir și Adleman, care au implementat sistemul menționat anterior numit RSA, care, după cum vom vedea, se bazează pe aritmetică modulară și controlează sistemele de securitate actuale care guvernează comunicațiile prin internet.