Criptografie şi Securitatea Informaţiei. Aplicaţii.

David Naccache Emil Simion
Adela Mihăiţă Ruxandra-Florentina Olimid Andrei-George Oprina

Prefaţă

Intrând progresiv în era informaţiei, societăţile industrializate se găsesc în faţa unui paradox: pe de o parte, puterea şi influenţa Europei şi a Americii de Nord au crescut semnificativ, în principal datorită măiestriei modalităţilor prin care se controlează fluxurile de informaţii, precum şi valorii crescute a datelor procesate. Pe de altă parte, după cum au demonstrat-o deja criza Wikileaks sau viermele Stuxnet, apar noi ameninţări şi vulnerabilităţi care fac ca dependenţa noastră de sistemele informaţionale să fie crucială.

De aceea, dezvoltarea atacurilor cibernetice, precum şi disponibilitatea online a instrumentelor utilizate în activitatea de piraterie conduce la obiective strategice importante şi cultivă necesitatea de a pregăti experţi pentru acest domeniu.

Criptografia este peste tot în jurul tău. În timp ce tu citeşti aceste rânduri, în vecinătatea ta se transmit informaţii cifrate prin telefoane mobile, relee de pay-TV, precum şi routere wireless. Mediul în care trăim se schimbă într-un ritm alert. Această evoluţie este rezultatul progresului în domeniul tehnologiilor hardware şi al matematicii.

Criptografia aplicată s-a dezvoltat considerabil în ultimii ani, pentru a putea satisface cerinţele crescute de securitate ale diverselor domenii legate de tehnologia informaţiei, cum ar fi telecomunicaţiile, reţelistica, bazele de date, precum şi aplicaţiile de telefonie mobilă. Sistemele criptografice sunt din ce în ce mai complexe şi mai tehnice şi necesită din ce în ce mai multă putere de calcul (de exemplu schema de cifrare perfect homomorfă a lui Gentry). În plus, algoritmii criptografici trebuie utilizaţi împreună cu protocoale adecvate, a căror proiectare şi înţelegere necesită o analiză delicată.

Această carte vă oferă instrumentele necesare pentru a începe să vă dezvoltaţi aptitudinile în domeniul criptografiei. În timp ce citiţi aceste rânduri în limba română, străinul care sunt vă îndeamnă să realizaţi că unele dintre cele mai luminate minţi care au adus contribuţii acestui domeniu îşi aveau originile în spaţiul lingvistic şi cultural românesc. De exemplu, cel care a spart maşina de cifrat "Purple" a japonezilor, faptă care a dus la divulgarea secretelor diplomatice japoneze înainte de intrarea Americii în cel de-al doilea război mondial, provenea din oraşul Chişinău, Republica Moldova, oraş în care familia lui se mutase după plecarea din Bucureşti la sfârşitul anilor 1890. Ştiinţa secretelor are o lungă tradiţie în România, ţară care a fost nevoită constant să se bazeze pe propriile talente pentru a-şi păstra independenţa. Experţii au prezis că următoarele războaie vor începe în spaţiul cibernetic. Autorii acestei cărţi, care sunt pedagogi şi cercetători, au importanta datorie morală de a lăsa moştenire României astfel de talente vitale.

În trecut, am avut onoarea de a cunoaşte sau a fi mentorul unor cercetători şi studenţi români foarte talentaţi. Întotdeauna am fost uimit de creativitatea acestora, de dorinţa lor de a-şi atinge scopurile, precum şi de dăruirea pentru muncă. Sper că această carte va contribui la dezvoltarea continuă de asemenea talente, astfel încât domeniul ştiinţific căruia i-am dedicat o bună parte a vieţii mele să beneficieze de acest formidabil rezervor de talente.

Dacă sunteţi un student talentat şi interesat de studii doctorale în domeniu, nu ezitaţi să mă contactaţi pentru sfaturi.

Prof. David Naccache
Université Paris II, Pantheon-Assas, PRES Sorbonne Universités
Membru al laboratorului informatic al Ecole normale superiéure. Paris, Franţa

Cuvânt înainte

Lucrarea de faţă conţine aplicaţii practice abordate de autori în cadrul seminariilor ce se desfăşoară la disciplina *Criptografie şi Securitate*, la Facultatea de Matematică Informatică din cadrul Universităţii din Bucureşti, la masterul de *Securitatea Tehnologiei Informaţiei*, organizat de Academia Tehnică Militară, precum şi la masterul de *Teoria Codării şi Stocării Informaţiei*, organizat de Facultatea de Ştiinţe Aplicate din cadrul Universităţii Politehnica Bucureşti.

Această culegere de probleme este un prim pas în dezvoltarea colaborării dintre şcoala românească de criptologie şi şcoala franceză reprezentată în cazul de faţă de David Naccache, profesor la universitatea Pantheon-Assas Paris II. Din acest motiv se regăsesc, în culegerea de faţă, capitolele dedicate principiilor criptologice şi atacurilor în mediul de implementare, ce acoperă un gol din curricula sistemului de învăţământ din Romania, capitole elaborate în colaborare cu profesorul David Naccache.

Materialul este structurat în capitole independente, fiecare capitol fiind constituit din trei părţi: prezentarea metodei (breviar teoretic), exemple de aplicare şi probleme propuse spre rezolvare, pentru fiecare dintre acestea indicându-se rezultatul ce trebuie obţinut.

Întrucât criptografia este o disciplină computaţională, autorii au considerat utilă introducerea unui capitol special dedicat aplicaţiilor software care pot constitui logistica necesară desfăşurării în bune condiţii a laboratoarelor la această disciplină.

În continuare considerăm util să definim unele dintre principalele noţiuni utilizate în cadrul acestei culegeri de probleme.

Criptologia este ştiinţa scrierilor secrete, având drept obiect apărarea secretului datelor şi informaţiilor confidenţiale, cu ajutorul sistemelor criptografice.

Criptografia este latura defensivă a *criptologiei*, având drept obiect de activitate elaborarea (conceperea) sistemelor criptografice şi a regulilor folosite.

Criptanaliza este latura ofensivă a *criptologiei*, având drept obiect de activitate studierea sistemelor criptografice proprii pentru a le oferi caracteristicile necesare, astfel încât acestea să-şi îndeplinească funcţia pentru care au fost concepute. Totodată criptanaliza poate analiza sistemele criptografice ale terţelor părţi (prin intermediul criptogramelor realizate cu ele) astfel încât prin spargerea acestora să obţină informaţii utile instituţiei pe care o deserveşte.

Prin *algoritm criptografic* înţelegem o mulţime de transformări uniinversabile prin care mulţimea mesajelor (textelor) clare dintr-o limbă se transformă în mulţimea $\mathcal{M}$ a criptogramelor.

Cheia de cifrare constituie o convenţie particulară, materializată, printr-un cuvânt, frază, număr, şir numeric etc. şi care dirijează (reglementează) *operaţia de cifrare*.

Un *protocol criptografic* este un set de reguli, între doi sau mai mulţi parteneri, prin intermediul căruia are loc o operaţie de autentificare şi/sau transfer de cheie sau mesaje.

Un *sistem criptografic* este compus din trei elemente: algoritm de cifrare, sistem de generare al cheilor şi protocol de distribuţie al cheilor de cifrare.

Descifrarea este operaţia inversă cifrării şi ea constă în aplicarea sistemului de cifrare cunoscut (în prezenţa cheii corecte) asupra criptogramelor pentru aflarea mesajului clar.

Decriptarea este operaţia prin care, numai pe baza analizei criptogramelor realizate cu un sistem de cifru necunoscut, se pune în evidenţă mesajul clar care a fost criptografiat şi se determină caracteristicile sistemului criptografic folosit pentru cifrare.

Dr. mat. Emil Simion

Cuprins

Capitolul 1

Sistemul de cifrare Cezar

1.1 Breviar teoretic

Algoritmul de cifrare al lui Cezar este un sistem de cifrare monoalfabetic pentru care textul clar este construit din literele alfabetului latin $A-Z$ şi cheia de cifrare este reprezentată de un număr întreg $k \in \{0, \ldots, 25\}$.

În faza de preprocesare, delimitatorul de spaţiu este ignorat sau înlocuit cu caracterul cel mai puţin frecvent din limba în care este textul clar (în limba română Q).

Fiecarei litere din textul sursă i se asociază ordinea lexicografică x. Pentru cifrare, aceasta se înlocuieşte prin caracterul cod $(x + k) \bmod 26$. Pentru descifrare se utilizează regula inversă: $(x - k) \bmod 26$.

1.2 Exerciţii rezolvate

Exerciţiul 1.2.1 *Să se cifreze mesajul:*
CRIPTOGRAFIE
algoritmul utilizat fiind cifrul lui Cezar cu cheia de cifrare $k = 7$.

Rezolvare: Se cifrează literă cu literă, ţinând cont de poziţia ocupată de litere în alfabet:
- Literei C îi corespunde $x = 2$, deci se va cifra în $(2 + 7) \bmod 26 = 9$ adică J;
- Literei R îi corespunde $x = 16$, deci se va cifra în $(17 + 7) \bmod 26 = 24$, adică Y;
Se continuă în mod analog pentru fiecare literă şi în final se obţine JYPWA VNYHM PL.

Exerciţiul 1.2.2 *Să se decripteze mesajul:*
JAJSN SHWDU YTQTL DXNQJ SHJNX LTQIJ SXXXX
algoritmul utilizat fiind cifrul lui Cezar. Indicaţi cheia de cifrare.

Rezolvare: Se verifică, pe rând, toate cheile posibile, până când se obţine un text cu sens.
În funcţie de lungimea cheii, corespondenţa dintre literele textului clar şi cele ale textului cifrat devine:

x	0	1	2	3	4	5	6	...	25
textul clar	A	B	C	D	E	F	G	...	Z
$k = 1$	B	C	D	E	F	G	H	...	A
$k = 2$	C	D	E	F	G	H	I	...	B
$k = 3$	D	E	F	G	H	I	J	...	C
$k = 4$	E	F	G	H	I	J	K	...	D
$k = 5$	F	G	H	I	J	K	L	...	E
...	..	..	..	..	..	..	..	..	..

Se observă că sistemul presupune înlocuirea fiecărei litere cu litera corespunzătoare în alfabetul rotit cu k poziţii.

Decriptând fiecare caracter în corespondentul său clar se obţine, pe rând:

- pentru $k = 1$: IZIRM RGVCT XSPSK CWMPI RGIMW KSPHI RWWWW
- pentru $k = 2$: HYHQL QFUBS WRORJ BVLOH QFHLV JROGH QVVVV
- pentru $k = 3$: GXGPK PETAR VQNQI AUKNG PEGKU IQNFG PUUUU
- pentru $k = 4$: FWFOJ ODSZQ UPMPH ZTJMF ODFJT HPMEF OTTTT
- pentru $k = 5$: EVENI NCRYP TOLOG YSILE NCEIS GOLDE NSSSS

După o regrupare a literelor, pentru $k = 5$ se obţine: EVEN IN CRYPTOLOGY SILENCE IS GOLDEN.

1.3 Exerciţii propuse

Exerciţiul 1.3.1 *Să se cifreze mesajul:*
MIRACLE
algoritmul utilizat fiind cifrul lui Cezar, cheia de cifrare $k = 3$.

Răspuns: PLUDFOH.

Exerciţiul 1.3.2 *Să se decripteze mesajul:*
IGQTI GYCUJ KPIVQ PXXXX
algoritmul utilizat fiind cifrul lui Cezar. Indicaţi cheia de cifrare.

Răspuns: GEORGE WASHINGTON, $k = 2$.

Capitolul 2

Metoda substituţiei

2.1 Breviar teoretic

Operaţia de cifrare se bazează pe o *corespondenţă* biunivocă între *alfabetul clar* şi *alfabetul cifrat*. Se presupune că alfabetul clar este format din cele 26 de litere (în limba română fără diacritice) plus *delimitatorul de cuvânt* spaţiul. Alfabetul cifrat poate fi format din aceeleaşi caractere sau doar din cele 26 de litere (ale limbii române) caz în care spaţiul se va înlocui cu cea mai puţin frecventă literă (Q) sau se va ignora pur şi simplu. În continuare, delimitatorul de cuvânt este înlocuit cu litera Q.

Corespondenţa dintre cele două alfabete poate fi:

- aleatoare;

- pseudoaleatoare: plecând de la o parolă se construieşte alfabetul cifrat.

Întrucât în cazul corespondenţei aleatoare lucrurile sunt cât se poate de clare, vom prezenta pe scurt o metodă de construcţie a corespondenţei în cel de-al doilea caz. Pornind de la o parolă, alfabetul cifrat este construit după următorul algoritm:

- se scriu, o singură dată, în ordinea apariţiei, literele din parolă;

- se scriu literele alfabetului care nu apar în parolă.

Corespondenţa între cele două alfabete se realizează după regula alfabet în alfabet după o permutare fixă σ (aceasta poate fi chiar permutarea identică iar la descifrare se aplică aceelaşi procedeu dar cu inversa permutării σ).

În funcţie de forma permutării substituţia se numeşte:

- *directă* (alfabetul cifrat are acelaşi sens lexicografic cu alfabetul clar, sunt în total 26 astfel de substituţii). Exemplu de substituţie directă:

A	B	C	D	E	F	G	H	I	J	K	L	M
G	H	I	J	K	L	M	N	O	P	Q	R	S

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C	D	E	F

- *inversă* (alfabetul cifrat are sens invers lexicografic cu alfabetul clar, sunt în total 26 de astfel de substituţii). Exemplu de substituţie inversă:

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

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

Reamintim aici trei exemple celebre (vechile coduri ebraice) de substituţii reciproce (dacă litera $\mathcal{X}$ se substituie cu litera $\mathcal{Y}$ atunci $\mathcal{Y}$ se va substitui cu $\mathcal{X}$) şi anume:

- *atbash* (prima jumătate a literelor alfabetului se mapează în cea de-a două jumătate în ordine invers lexicografică):

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

- *albam* (prima jumătate a literelor alfabetului se mapează în cea de-a două jumătate în ordine lexicografică):

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

- *atbah*:

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

În cele ce urmează vom presupune faptul că substituţia este directă dacă nu este specificat altfel.

Definiţia 2.1 *Un* **cifru de substituţie liniar** *de la* $\mathbf{Z}_m$ *la* $\mathbf{Z}_m$ *(*m *fiind numărul de caractere al alfabetului sursă) poate fi descris prin funcţia* $f : \mathbf{Z}_m \to \mathbf{Z}_m$ *definită prin* $f(x) = \alpha x + \beta$ *cu* $\gcd(\alpha, m) = 1$, *funcţia de descifrare fiind* $f^{-1}(x) = \alpha^{-1}(x - \beta)$. *Cheia de cifrare o formează numerele* α *şi* β.

Observaţia 2.1 *Cifrul de substituţie are proprietatea de confuzie (ascunderea legăturii dintre textul clar şi textul cifrat).*

2.2 Exerciţii rezolvate

Exerciţiul 2.2.1 *Să se construiască alfabetul de cifrare cu ajutorul parolei*

$$TESTARESISTEM$$

iar apoi să se cifreze mesajul IN CRIPTOGRAFIE NICI O REGULA NU ESTE ABSOLUTA. Permutarea care realizează corespondenţa este:

0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
25	*24*	*23*	*22*	*21*	*20*	*19*	*18*	*17*	*16*	*15*	*14*	*13*

13	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*
12	*11*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*

Rezolvare:

Corepondenţa dintre alfabetul clar şi alfabetul de cifrare (înainte de realizarea permutării) este:

A	B	C	D	E	F	G	H	I	J	K	L	M
T	E	S	A	R	I	M	B	C	D	F	G	H

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	N	O	P	Q	U	V	W	X	Y	Z

Corepondenţa dintre alfabetul clar şi alfabetul de cifrare după realizarea permutării este:

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

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

Mesajul clar se procesează astfel încât spaţiul este înlocuit cu cea mai puţin frecventă literă:

$$INQCRIPTOGRAFIEQNICIQOQREGULAQNUQESTEQABSOLUTA.$$

Mesajul cifrat va fi:
OHDXC OFMGQ CZUOV DHOXO DGDCV QIKZD HIDVB MVDZY BGKIM Z.

Exerciţiul 2.2.2 *Să se descifreze mesajul:*
DOJMD OVPGF OMATN BXXXX
algoritmul utilizat fiind o substituţie simplă determinată de cuvântul cheie PASSWORD.

Rezolvare:

Corespondenţa dintre alfabetul clar şi alfabetul de cifrare este:

A	B	C	D	E	F	G	H	I	J	K	L	M
P	A	S	W	O	R	D	B	C	E	F	G	H

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	J	K	L	M	N	Q	T	U	V	X	Y	Z

Mesajul clar devine (dupa o regrupare a literelor) GEORGE WALKER BUSH. Se observă că de această dată nu s-a mai folosit Q pe post de delimitator de cuvânt.

2.3 Exerciţii propuse

Exerciţiul 2.3.1 *Să se cifreze mesajul:*
WEB DESIGN
algoritmul utilizat fiind o substituţie simplă determinată de cuvântul cheie BROWSER.

Răspuns: VSRWS PDAJ.

Exerciţiul 2.3.2 *Să se descifreze mesajul:*
ONCJB DFJPT DCJKN KKQTV TDSXXX
algoritmul utilizat fiind o substituţie simplă determinată de cuvântul cheie CRIPTOGRAFIE.

Răspuns: FRANKLIN DELANO ROOSEVELT.

Capitolul 3

Sistemul de cifrare Playfair

3.1 Breviar teoretic

Sistemul *Playfair*, propus în anul 1854 de Charles Wheatstone dar promovat pentru utilizare de Lordul Playfair, este unul dintre cele mai cunoscute sisteme de cifrare digrafice (transformă un grup de 2 litere într-un grup de alte două litere). Acest sistem de cifrare este foarte simplu de folosit şi mult mai sigur decât sistemele de substituţie monoalfabetice.

Descriem în continuare modul de utilizare în cazul alfabetului latin compus din 26 litere. Literele alfabetului $A - Z$ sunt trecute într-un careu de 5×5 (litera I fiind asimilată literei J). Textul clar este preprocesat astfel încât acesta să fie compatibil cu matricea de cifrare: delimitatorul de cuvânt este ignorat sau este înlocuit cu cea mai puţin frecventă literă, litera I este asimilată cu litera J, şi dacă este cazul, se adaugă o literă la text pentru a avea un număr par de digrame.

Regula de cifrare este următoarea:

i) Dacă digrama care se doreşte cifrată nu are literele pe aceeaşi linie sau coloană, atunci regula de cifrare este *regula dreptunghiului*, traseul fiind pe verticală de la cea de-a doua literă a digramei către prima literă. Sau, altfel spus, prima litera a perechii cifrate este aceea care se gaseste pe aceeasi linie cu prima litera a perechii în clar.

ii) Dacă digrama ce se doreşte cifrată are literele pe aceeaşi linie, atunci se aplică regula: *cifrează la dreapta, descifrează la stânga.*

iii) Dacă digrama ce se doreşte cifrată are literele pe aceeiaşi coloană, atunci se aplică regula: *cifrează în jos, descifrează în sus.*

Observaţia 3.1 *Dacă o digramă apare în textul clar în ordine inversă atunci acelaşi lucru se va întâmpla şi în textul cifrat.*

Observaţia 3.2 *Algoritmul Playfair nu are regulă pentru cifrarea literelor duble: digramele ce conţin două litere identice sunt sparte prin introducerea artificială a unei alte litere.*

Observaţia 3.3 *Algoritmul Playfair apare ca o extindere, în sensul reducerii numărului de tabele rectangulare folosite (de la două la unul), al cifrului cu* 2 *tabele.*

Metoda cea mai freventă de atac a acestui tip de cifru constă în analiza frecvenţei digramelor de text clar combinată cu metoda comparaţiei patternurilor din textul cifrat cu patternuri din dicţionar.

3.2 Exerciţii rezolvate

Exerciţiul 3.2.1 *Să se construiască matricea de cifrare Playfair cu ajutorul parolei*

$$CRIPTOGRAFIE$$

iar apoi să se cifreze mesajul SI IN CRIPTOGRAFIE TACEREA ESTE AUR.

Rezolvare: Matricea Playfair se obţine trecând literele din parolă o singură dată în careul de 5×5 iar apoi celelalte litere ale alfabetului în ordine lexicografică:

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

Mesajul este preprocesat, prin introducerea literei Q ca delimitator de cuvânt şi la finalul mesajului (pentru ca acesta să aibă lungime pară):

$$SIQINQCRIPTOGRAFIEQTACEREAQESTEQAURQ.$$

Exemplificăm pentru fiecare caz câte o digramă:

- SI - conform regulii de cifrare se formează dreptunghiul cu colţurile I şi S parcurs în sensul IQSP. Textul cifrat îl constituie digrama formată din colţurile care nu apar în textul clar, luate conform ordinii de parcurgere: QP.
- QI - întrucât literele sunt pe aceeaşi coloană se aplică regula cifrează în jos, descifrează în sus, obţinându-se digrama XA (X este litera situată sub Q şi A este litera situată sub I).
- NQ - întrucât literele sunt situate pe aceeaşi linie se aplică regula cifrează la dreapta, descifrează la stânga, obţinându-se digrama QS(Q este in dreapta lui N şi S este în dreapta lui Q).

În continuare, respectând regulile de cifrare Playfair mesajul cifrat devine:
QPXAQ SRIPT CEDGF ETAUI OIGTO FUAUP AUEQI NXXXX.

Exerciţiul 3.2.2 *Să se descifreze mesajul:*
UFRIL ERGPC RQAW
Algoritmul utilizat este cifrul lui Playfair, parola utilizată fiind CRIPTOGRAFIE.

Rezolvare: Matricea Playfair este aceeaşi din exerciţiul anterior, fiind formată pornind de la aceeaşi parolă.

Exemplificăm pentru fiecare caz operaţia de descifrare pe câte o digramă:

- UF - conform regulii de descifrare, se formează dreptunghiul cu colţurile U şi F. Textul clar îl constituie celelalte 2 colţuri, primul caracter al textului clar fiind cel care se găseşte pe aceeaşi linie cu primul caracter în clar din digramă. Se obţine SE.
- RI - întrucât literele sunt situate pe aceeaşi linie se aplică regula cifrează la dreapta, descifrează la stânga, obţinându-se digrama CR(R este in stânga lui R şi R este în stânga lui I).
- LE - întrucât literele sunt pe aceeaşi coloană se aplică regula cifrează în jos, descifrează în sus, obţinându-se digrama ET (E este litera situată deasupra lui L şi T este litera situată deasupra lui E).

  În continuare, respectând regulile de descifrare Playfair mesajul cifrat devine:

  SECRET WRITING.

3.3 Exerciţii propuse

Exerciţiul 3.3.1 *Să se cifreze mesajul:*
SECURITY IS CHANGING FIELD
Algoritmul utilizat este cifrul lui Playfair, parola utilizată fiind CHANNEL.

Răspuns: UAEQQ KYNMQ HANEL PEFLO CGMA.

Exerciţiul 3.3.2 *Să se descifreze mesajul:*
KDDPM RUBVR PTSFU HPEBV
Algoritmul utilizat este cifrul lui Playfair, parola utilizată fiind PASSWORD.

Răspuns: GERALD RUDOLPH FORD.

Capitolul 4

Sistemul de cifrare Hill

4.1 Breviar teoretic

Sistemul de cifrare Hill este o metodă de substituţie poligrafică bazată pe calcule efectuate în algebra mod p.

În faza de preprocesare delimitatorul de spaţiu este ignorat sau înlocuit cu caracterul cel mai puţin frecvent din limba în care este textul clar (în limba română Q).

Algoritmul procesează un bloc de date $\mathbf{M}$ de n caractere (litere), cheia de cifrare fiind reprezentată de o matrice $\mathbf{K}$ de dimensiune $n \times n$, inversabilă mod p.

Există două subclase ale algoritmului Hill pentru care regulile de cifrare diferă prin ordinea în care se efectuează înmulţirile: o prima subclasa are ca regulă de cifrare operaţia de înmulţire $\mathbf{C} = \mathbf{MK}$ cu descifrarea $\mathbf{M} = \mathbf{CK}^{-1}$ iar a doua subclasa foloseşte ca regulă de cifrare înmulţirea $\mathbf{C} = \mathbf{KM}$ având descifrarea corespunzătoare $\mathbf{M} = \mathbf{K}^{-1}\mathbf{C}$.

Observaţia 4.1 *Dacă matricea* $\mathbf{K}$ *este simetrică (matricea* $\mathbf{K}$ *şi transpusa ei sunt egale) atunci regulile de cifrare pentru cele două subclase sunt echivalente.*

Observaţia 4.2 *În cazul alfabetului latin* $p = 26$*, cheia de cifrare* $\mathbf{K}$ *trebuie să fie o matrice inversabilă mod* 26*.*

4.2 Exerciţii rezolvate

Exerciţiul 4.2.1 *Să se cifreze mesajul:*

BLAZE OF GLORY.

Algoritmul utilizat este cifrul lui Hill (2×2*), cheia de cifrare fiind matricea:*

$$\begin{pmatrix} J & B \\ V & I \end{pmatrix}.$$

Rezolvare: Prin înlocuirea literelor din cheie cu poziţiile corespunzătoare din alfabet (A - 0, B - 1, etc.) se obţine:

$$\mathbf{K} = \begin{pmatrix} 9 & 1 \\ 21 & 8 \end{pmatrix}.$$

Textul clar se sparge în blocuri de 2 caractere, care se cifrează pe rând. De exemplu, BL corespunde matricii

$$\mathbf{M} = \begin{pmatrix} 1 & 11 \end{pmatrix}.$$

Digrama se cifrează în:

$$\mathbf{C} = \begin{pmatrix} 1 & 11 \end{pmatrix} \begin{pmatrix} 9 & 1 \\ 21 & 8 \end{pmatrix} \bmod 26 = \begin{pmatrix} 6 & 11 \end{pmatrix} = \begin{pmatrix} G & L \end{pmatrix}.$$

Deci, BL se cifrează în GL. Se continuă în mod analog. În final se obţine:
GLFSS MPBDT HB.

Exerciţiul 4.2.2 *Să se descifreze mesajul:*
JESHB JJAZM TANCF VBJXX.
Algoritmul utilizat este cifrul lui Hill (2×2), cheia de cifrare fiind matricea:

$$\begin{pmatrix} H & U \\ D & F \end{pmatrix}.$$

Rezolvare: Prin înlocuirea literelor din cheie cu poziţiile corespunzătoare din alfabet (A - 0, B - 1, etc.) se obţine:

$$\mathbf{K} = \begin{pmatrix} 7 & 20 \\ 3 & 5 \end{pmatrix}.$$

Se determină inversa matricei K mod 26 :

$$\mathbf{K}^{-1} = det(\mathbf{K})^{-1}\mathbf{K}^{*} \bmod 26, unde$$

$$det(\mathbf{K})^{-1} \bmod 26 = (7 \cdot 5 - 3 \cdot 20)^{-1} \bmod 26 = (-25)^{-1} \bmod 26 = 1$$

şi

$$\mathbf{K}^{*} = \begin{pmatrix} 5 & -20 \\ -3 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 6 \\ 23 & 7 \end{pmatrix}.$$

S-a obţinut:

$$\mathbf{K}^{-1} = \begin{pmatrix} 5 & 6 \\ 23 & 7 \end{pmatrix}.$$

Pentru descifrarea perechii JE, se determină matricea linie care conţine valorile corespunzătoare din alfabet:

$$\mathbf{C} = \begin{pmatrix} J & E \end{pmatrix} = \begin{pmatrix} 9 & 4 \end{pmatrix}.$$

Prin înmulţire cu cheia de descifrare se obţine:

$$\mathbf{M} = \begin{pmatrix} 9 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 23 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 & 4 \end{pmatrix} = \begin{pmatrix} H & E \end{pmatrix}.$$

Deci, JE se descifrează în HE.

Se procedează în mod analog pentru toate perechile de câte 2 caractere cifrate: SH se descifrează în RB, BJ în ER, etc.

În final, după efectuarea tuturor calculelor şi regruparea literelor, se obţine: HERBERT CLARK HOOVER.

4.3 Exerciţii propuse

Exerciţiul 4.3.1 *Să se cifreze mesajul:*
COMPLETE AND PROPER PACKAGE.
Algoritmul utilizat este cifrul lui Hill, cheia de cifrare fiind matricea:

$$\begin{pmatrix} N & T \\ C & R \end{pmatrix}.$$

Răspuns: GIZTL MLCNN MBTML UMDMI AUYC.

Exerciţiul 4.3.2 *Să se descifreze mesajul:*
ZKNAW NIOZO BRXSW QNNXX.
Algoritmul utilizat este cifrul lui Hill (2×2), cheia de cifrare fiind matricea:

$$\begin{pmatrix} B & E \\ V & H \end{pmatrix}.$$

Răpuns: RONALD WILSON REAGAN.

Capitolul 5

Sisteme de cifrare polialfabetice

5.1 Breviar teoretic

Un sistem de cifrare de tip substituţie polialfabetică este generalizarea sistemului de cifrare de substituţie monoalfabetică, fiind compus dintr-un număr N de alfabete. Fiecare alfabet reprezintă o permutare (stabilită în funcţie de parolă) a alfabetului de intrare. Algoritmul de cifrare constă în substituirea celei de a $i-$a litere m din textul clar cu litera corespunzătoare din cel de al $i \bmod N$ alfabet.

Sistemele polialfabetice sunt uşor de identificat prin aplicarea analizei frecvenţelor de apatiţie a literelor în secvenţe decimate din textul cifrat.

Un exemplu de sistem polialfabetic este algoritmul lui Vigenère în care parola $k_1, \ldots, k_n$ este folosită periodic pentru a transforma caracterul $m_j \in \{A, \ldots, Z\}$ din textul clar după formula: $c_j = (m_j + k_{j \bmod n}) \bmod 26$. Pentru descifrare se foloseşte formula: $m_j = (c_j - k_{j \bmod n}) \bmod 26$.

Atacul sistemelor polialfabetice este similar cu atacul a N sisteme de substituţie monoalfabetică. Deci, o procedură de *tip divide et impera* are o complexitate de $O(N)$. Procedura este descrisă în continuare:

Intrare: Textul cifrat de lungime M suficient de mare.

Ieşire: Textul clar corespunzător sistemului de cifrare polialfabetic.

PASUL 1. Determină numărul de alfabete N.

PASUL 2. Pentru $j = 0$ to 4 execută:

pentru $i = 1$ to $N - j$ execută:

aplică procedura de reconstrucţie parţială (pe baza frecvenţelor $(j+1)-$gramelor) a alfabetelor $i, \ldots, i + j$.

PASUL 3. Conform celor N alfabete reconstruieşte textul clar.

Observaţia 5.1 *Procedura descrisă mai sus are ca parametru implicit de analiză numărul maxim de legături* 4 : *astfel,* $1-$*gramele sunt caracterele,* $2-$*gramele sunt dubleţii, etc.*

5.2 Exerciţii rezolvate

Exerciţiul 5.2.1 *Să se cifreze mesajul WINDS OF CHANGE cu ajutorul algoritmului Vigenère, parola fiind FUTURE.*

Rezolvare: Aplicând cifrarea pentru fiecare caracter al textului clar, ţinând cont de poziţia acestora în alfabet, se obţine:

$\mathbf{j}$	$\mathbf{m_j}$	$\mathbf{k_{j(mod\,6)}}$	$\mathbf{c_j = (m_j + k_{j(mod\,6)})(mod\,26)}$
1	$W-22$	$F-5$	$(22+5)(mod\,26) = 1-B$
2	$I-8$	$U-20$	$(8+20)(mod\,26) = 2-C$
3	$N-13$	$T-19$	$(13+19)(mod\,26) = 6-G$
4	$D-3$	$U-20$	$(3+20)(mod\,26) = 23-X$
5	$S-18$	$R-17$	$(18+17)(mod\,26) = 9-J$
6	$O-14$	$E-4$	$(14+4)(mod\,26) = 18-S$
7	$F-5$	$F-5$	$(5+5)(mod\,26) = 10-K$
8	$C-2$	$U-20$	$(2+20)(mod\,26) = 22-W$
9	$H-7$	$T-19$	$(7+19)(mod\,26) = 0-A$
10	$A-0$	$U-20$	$(0+20)(mod\,26) = 20-U$
11	$N-13$	$R-17$	$(13+17)(mod\,26) = 4-E$
12	$G-6$	$E-4$	$(6+4)(mod\,26) = 10-K$
13	$E-4$	$F-5$	$(4+5)(mod\,26) = 9-J$

Rezultă textul cifrat: BCGXJ SKWAU EKJ.

Exerciţiul 5.2.2 *Să se descifreze mesajul IHWGZ CIHGO GKAJV OI ştiind că a fost cifrat cu ajutorul algoritmului Vigenère, parola fiind PASSWORD.*

Rezolvare: Aplicând descifrarea pentru fiecare caracter al textului cifrat, ţinând cont de poziţia acestora în alfabet, se obţine:

$\mathbf{j}$	$\mathbf{c_j}$	$\mathbf{k_{j(\mathrm{mod}\,8)}}$	$\mathbf{m_j = (c_j - k_{j(\mathrm{mod}\,8)})(\mathrm{mod}\,26)}$
1	$I-8$	$P-15$	$(8-15)(mod\,26) = 19-T$
2	$H-7$	$A-0$	$(7-0)(mod\,26) = 7-H$
3	$W-22$	$S-18$	$(22-18)(mod\,26) = 4-E$
4	$G-6$	$S-18$	$(6-18)(mod\,26) = 14-O$
5	$Z-25$	$W-22$	$(25-22)(mod\,26) = 3-D$
6	$C-2$	$0-14$	$(2-14)(mod\,26) = 14-O$
7	$I-8$	$R-17$	$(8-17)(mod\,26) = 17-R$
8	$H-7$	$D-3$	$(7-3)(mod\,26) = 4-E$
9	$G-6$	$P-15$	$(6-15)(mod\,26) = 17-R$
10	$O-14$	$A-0$	$(14-0)(mod\,26) = 14-O$
11	$G-6$	$S-18$	$(6-18)(mod\,26) = 14-O$
12	$K-10$	$S-18$	$(10-18)(mod\,26) = 18-S$
13	$A-0$	$W-22$	$(0-22)(mod\,26) = 4-E$
14	$J-9$	$0-14$	$(9-14)(mod\,26) = 21-V$
15	$V-21$	$R-17$	$(21-17)(mod\,26) = 4-E$
16	$O-14$	$D-3$	$(14-3)(mod\,26) = 11-L$
17	$I-8$	$P-15$	$(8-15)(mod\,26) = 19-T$

Dupa gruparea literelor rezultă: THEODORE ROOSEVELT.

5.3 Exerciţii propuse

Exerciţiul 5.3.1 *Să se cifreze mesajul OPTIMISTIC cu ajutorul algoritmului Vigenère, folosind parola GOODDAYS.*

Răspuns: UDHLPIQLOQ.

Exerciţiul 5.3.2 *Să se descifreze mesajul WIUXGHG WXGALFYK ştiind că a fost cifrat cu ajutorul algoritmului Vigenère, parola fiind TEST.*

Răspuns: DECENDO DECISMUS.

Capitolul 6

Metoda transpoziţiei

6.1 Breviar teoretic

Metoda transpoziţiei asigură, în cadrul sistemelor criptografice, realizarea difuziei: împrăştierea proprietăţilor statistice ale textului clar în textul cifrat. Metoda transpoziţiei îmbracă mai multe forme: textul *este citit* într-o formă matriceală linie cu linie sau coloană cu coloană, *se permută* liniile şi/sau coloanele, rezultatul fiind apoi *scris* linie cu linie sau coloană cu coloană. Spre exemplu, în cazul transpoziţiei coloanelor, textul clar se citeşte, linie cu linie, într-o formă tabelară cu n coloane, acesta fiind scris pe coloane în funcţie de cheia de cifrare reprezentată de o permutare din σ_n.

Dacă dimensiunea textului clar nu este un multiplu de n atunci acesta se poate completa sau nu cu un caracter bine precizat. În faza de preprocesare delimitatorul de spaţiu este ignorat sau înlocuit cu caracterul cel mai puţin frecvent din limba în care este textul clar (în limba română Q).

6.2 Exerciţii rezolvate

Exerciţiul 6.2.1 *Să se cifreze prin metoda transpoziţiei* ($N = 12$), *pornind de la parola*

$$CRIPTOGRAFIE$$

mesajul SI IN CRIPTOGRAFIE TACEREA ESTE AUR.

Rezolvare: Vom construi secvenţa numerică de cifrare asociind fiecărei litere din parolă indicele din ordinea lexicografică: astfel literele din parolă, scrise în ordine lexicografică sunt:

1	2	3	4	5	6	7	8	9	10	11	12
A	C	E	F	G	I	I	O	P	R	R	T

deci parola $CRIPTOGRAFIE$ produce permutarea: 2 10 6 9 12 8 5 11 1 4 7 3.

Textul clar este scris într-o tabelă cu 12 coloane:

2	10	6	9	12	8	5	11	1	4	7	3
S	I	Q	I	N	Q	C	R	I	P	T	O
G	R	A	F	I	E	Q	T	A	C	E	R
E	A	Q	E	S	T	E	Q	A	U	R	Q

Deoarece lungimea textului nu este divizibilă cu 12 vom completa ultimul rând cu o secvenţă cunoscută (în acest caz caracterul Q). Textul cifrat se obţine citind coloanele tabelei de cifrare în ordinea indicată de parola numerică: IAASG EORRQ PCUCQ EQAQT ERQET IFEIR ARTQN IS.

Descifrarea se va realiza în mod similar folosind permutarea inversă σ^{-1}.

Dacă dimensiunea transpoziţiei N este mai mică decât lungimea parolei atunci se vor reţine N caractere din parolă.

6.3 Exerciţii propuse

Exerciţiul 6.3.1 *Să se cifreze mesajul:*
ELECTRIC HOTPLATE
printr-o transformare de tip transpoziţie cu ajutorul permutării $\sigma = (2, 1, 3)$.

Răspuns: LTCOL EECIH PTERQ TAQ.

Exerciţiul 6.3.2 *Să se descifreze mesajul:*
EORSE TOROE LHDEO VT
cifrat printr-o transformare de tip transpoziţie cu ajutorul permutării $\sigma = (2, 3, 1)$.

Răspuns: THEODORE ROOSEVELT.

Capitolul 7

Sisteme mixte

7.1 Breviar teoretic

Sistemele mixte au la bază o cifrare succesivă a mesajului prin metoda substituţiei şi apoi prin metoda transpoziţiei sau invers.

Atacarea sistemul de cifrare se realizează de la ultima sa componentă către prima. Remarcăm faptul că substituţia simplă este comutativă cu operaţia de transpoziţie deci se poate oricând aborda mai întâi substituţia şi apoi transpoziţia. În cazul utilizării unui sistem polialfabetic, cu număr necunoscut de alfabete, recomandarea este ca după stabilirea, prin metode statistice, a numărului de alfabete, să se abordeze concomitent identificarea efectivă a alfabetelor şi al transpoziţiei utilizate. În cazul utilizării unui sistem poligrafic (tabele de cifrare) şi o transpoziţie este recomandabilă o tehnică de tip backtracking.

7.2 Exerciţii rezolvate

Exerciţiul 7.2.1 *Să se cifreze mesajul GEOMETRIC FIGURE cu ajutorul algoritmului lui Cezar ($k = 5$) şi al transpoziţiei $\sigma = (2, 1, 3)$.*

Rezolvare: Mai întâi textul este cifrat cu sistemul Cezar folosind cheia $k = 5$, deci corespondenţa dintre cele 2 alfabete devine:

text clar	A	B	C	D	E	F	G	H	I	...
text cifrat	F	G	H	I	J	K	L	M	N	...

Astfel se obţine: LJT RJY WNH KNL ZWJ. Apoi, textul obţinut se aşează într-o tabelă cu 3 coloane:

2	1	3
L	J	T
R	J	Y
W	N	H
K	N	L
Z	W	J

Textul cifrat se determină citind pe coloane în ordinea indicată de permutare (coloana din mijloc, apoi cea din stânga şi în final cea din dreapta): JJNNWLRW KZTYHLJ .

Exerciţiul 7.2.2 *Să se decripteze mesajul următor:*

DKVUR UTUBK WFCVG ETGOC XWVWC

OCVPQ VUVWG FGHTQ VKUUV KKNKC

RKCPQ OQFKC EWVG

ştiind că a fost cifrat cu ajutorul algoritmului lui Cezar ($k = 2$) şi supracifrat prin metoda transpoziţiei utilizând permutarea $(3, 2, 1)$.

Rezolvare: Cum substituţia şi transpoziţia sunt comutative, putem mai întâi decripta mesajul folosind Cezar cu cheia $k = 2$ şi apoi decripta prin metoda transpoziţiei.

Pentru decriptarea mesajului folosind metoda Cezar cu $k = 2$, fiecare caracter se înlocuieşte cu caracterul situat cu 2 poziţii mai înainte în alfabet:

text cifrat	A	B	C	D	E	F	G	H	I	...
text clar	Y	Z	A	B	C	D	E	F	G	...

După decriptare, textul devine: BITSP SRSZI UDATE CREMA VUTUA MATNO TSTUE DEFRO TISST IILIA PIANO MODIA CUTE .

Acesta reprezintă un text cifrat prin metoda transpoziţiei. Cum textul are 64 de caractere şi permutarea este de lungime 3, atunci numărul de litere pe coloane este: 21, 21 şi 22. Coloanele cu numai 21 de caractere sunt cele care corespund valoriilor luate în ordine descrescătoare din permutarea inversă $\sigma^{-1} = (3, 2, 1)$:

3	2	1
B	U	S
I	T	S
T	U	T
S	A	I
P	M	I
S	A	L
R	T	I
S	N	A
Z	O	P
I	T	I
U	S	A
D	T	N
A	U	O
T	E	M
E	D	O
C	E	D
R	F	I
E	R	A
M	O	C
A	T	U
V	I	T
		E

1	2	3
S	U	B
S	T	I
T	U	T
I	A	S
I	M	P
L	A	S
I	T	R
A	N	S
P	O	Z
I	T	I
A	S	U
N	T	D
O	U	A
M	E	T
O	D	E
D	E	C
I	F	R
A	R	E
C	O	M
U	T	A
T	I	V
E		

După rearanjarea coloanelor conform permutării inverse σ^{-1} se obţine tabela din dreapta. Citind pe linii se descoperă textul clar: SUBSTITUTIA SIMPLA SI TRANSPOZITIA SUNT DOUA METODE DE CIFRARE COMUTATIVE .

7.3 Exerciţii propuse

Exerciţiul 7.3.1 *Se dau criptogramele:*
Criptograma 1:
VXEVW LWXWL DVLPS ODVLW UDQVS
RCLWL DVXQW GRXDP HWRGH GHFLI
UDUHF RPXWD WLYHX
Criptograma 2:
YAHYZ OZAZO GYOSV RGYOZ XGTYV
UFOZO GYATZ JUAGS KZUJK JKIOL
XGXKI USAZG ZOBKX
Care din afirmaţiile de mai jos sunt adevărate:
a) metoda de cifrare utilizată este o substituţia simplă;
b) metoda de cifrare utilizată este o transpoziţie;

c) metoda de cifrare este reprezentată de algoritmul lui Cezar;
d) nu se poate preciza sistemul criptografic utilizat.
Justificaţi răspunsul. Decriptaţi mesajul.

Răspuns: a) şi c). Textul clar: SUBSTITUTIA SIMPLA SI TRANSPOZITIA SUNT DOUA METODE DE CIFRARE COMUTATIVE.

Exerciţiul 7.3.2 *Se dau criptogramele:*
Criptograma 1:
BITSP SRSZI UDATE CREMA VUTUA
MATNO TSTUE DEFRO TISST IILIA
PIANO MODIA CUTE
Criptograma 2:
UTUAM ATNOT STUED EFROT IBITS
PSRSZ IUDAT ECREM AVSST IILIA
PIANO MODIA CUTE
Care din afirmaţiile de mai jos sunt adevărate:
a) metoda de cifrare utilizată este o substituţia simplă;
b) metoda de cifrare utilizată este o transpoziţie;
c) metoda de cifrare este reprezentată de algoritmul lui Cezar;
d) nu se poate preciza sistemul criptografic utilizat.
Justificaţi răspunsul. Decriptaţi mesajul.

Răspuns: b). Textul clar: SUBSTITUTIA SIMPLA SI TRANSPOZITIA SUNT DOUA METODE DE CIFRARE COMUTATIVE.

Exerciţiul 7.3.3 *Cifraţi mesajul SPECIAL PROPERTY folosind algoritmului lui Cezar* ($k = 13$) *şi transpoziţia dată de* $\sigma = (2, 4, 3, 1)$.

Răspuns: PCRFVEE RYCLCNBG.

Exerciţiul 7.3.4 *Decriptaţi mesajul CPKQCG ZGTVTKGOERIH ştiind că a fost cifrat cu ajutorul algoritmului lui Cezar şi al unei transpoziţii.*

Răspuns: EXAMEN CRIPTOGRAFIE.

Capitolul 8

Generatoare pseudoaleatoare

8.1 Breviar teoretic

Un registru de deplasare cu feedback constă în n locaţii de memorie de câte un bit care se "deplasează" spre dreapta şi o funcţie de feedback care exprimă orice element nou $a(t)$, cu $t \geq n$, al secvenţei în funcţie de elementele generate anterior $a(t-n), a(t-n+1), \ldots, a(t-1)$.

Funcţia de feedback trebuie să fie nesingulară, adică de forma:

$a(t) = g(a(t-1), \ldots, a(t-n+1)) \oplus a(t-n)$, unde $\oplus$ desemnează operaţia SAU exclusiv (XOR). Dacă funcţia de feedback este liniară (se poate implementa doar folosind operaţia SAU exclusiv) spunem că generatorul este un registru de deplasare cu feedback liniar (**LFSR**). Altfel, spunem că generatorul este un registru de deplasare cu feedback neliniar (**NLFSR**).

O locaţie de memorie a registrului se numeşte nivel, iar semnalele binare $a(0), a(1), \ldots, a(n-1)$ sunt încărcate ca date iniţiale. Perioada secvenţei produse depinde atât de numărul de niveluri, cât şi de detaliile conexiunilor de feedback. Mai exact, perioada maximă a secvenţei care poate fi generată de un registru de deplasare cu feedback, având n niveluri şi o funcţie de feedback nesingulară este $2^n - 1$, adică numărul maxim de stări în care se poate afla un registru cu n niveluri (se exclude starea nulă). **LFSR**-urile sunt folosite de mult timp pentru teste **VSLI**, comunicaţii cu spectru distribuit etc. Funcţia de feedback a unui **LFSR** are forma:

$$a(t) = c_1 a(t-1) \oplus c_2 a(t-2) \oplus \ldots \oplus c_{n-1} a(t-n+1) \oplus a(t-n), \tag{8.1}$$

unde $c_i \in \{0, 1\}$. Conexiunea de feedback a unui **LFSR** poate fi exprimată printr-un polinom de feedback:

$$f(X) = 1 + c_1 X + c_2 X^2 + \ldots + c_{n-1} X^{n-1} + X^n,$$

cu nedeterminata X. Acest polinom decide perioada şi comportarea statistică a secvenţei de ieşire. Pentru a preveni o secvenţă de ieşire trivială, trebuie ca starea ,,zero peste tot" să nu

fie stare iniţială. De exemplu, dacă un **LFSR** cu patru niveluri are polinomul de feedback:

$$f(X) = 1 + X + X^2 + X^3 + X^4,$$

dependent de starea iniţială, atunci el va genera una din secvenţele de perioadă 5.

a) 1111011110 . . . ,

b) 1000110001 . . . ,

c) 0100101001 . . . ,

Sau, alt exemplu, dacă **LFSR** are polinomul de feedback dat de $f(X) = 1 + X + X^4$, atunci el generează o singură secvenţă netrivială de perioadă 15, cu cea mai bună statistică pe care o astfel de secvenţă o poate avea:

101100100011110 . . .

Pentru a garanta cea mai mare perioadă posibilă $2^n - 1$, polinomul de feedback $f(X)$ al **LFSR**-ului trebuie să fie *primitiv*. Aceasta însemnă că $f(X)$ trebuie ales astfel încât cel mai mic număr întreg pozitiv T pentru care $X^T - 1$ este divizibil cu $f(X)$ să fie $T = 2^n - 1$. Există algoritmi care testează primitivismul unui polinom. Numărul de polinoame primitive de grad n este:

$$N_p(n) = \frac{\Phi(2^n - 1)}{n},$$

unde $\Phi(x)$, cunoscută ca *funcţia lui Euler*, desemnează cardinalul de numere naturale mai mici ca x şi relativ prime cu x. Observăm că dacă un polinom $f(X)$ este primitiv atunci şi polinomul *reciproc* lui adică $X^n f(\frac{1}{X})$ este primitiv. Se ştie că orice polinom primitiv este ireductibil. Reciproca nu este adevărată. Numărul de polinoame ireductibile de grad n în algebra mod p ($p = 2$) este dat de formula următoare:

$$N_I(n) = \frac{1}{n} \sum_{d|n} p^d \mu(\frac{n}{d}),$$

unde μ este *funcţia lui Möebius* definită în felul următor pentru $n = \prod_1^k p_i^{\alpha_i}$: $\mu(n) = 0$ dacă $\prod_i^k \alpha_i > 1$, $\mu(n) = (-1)^k$ dacă n este produsul a k numere prime distincte şi $\mu(1) = 1$. Legătura între funcţia lui Moebius şi funcţia lui Euler este dată de:

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Dacă k este un *număr prim Mersenne*, adică k este număr prim de forma $2^n - 1$ unde n este număr prim, atunci orice polinom ireductibil de grad k (în algebra mod 2) este primitiv:

$$\begin{aligned} N_I(k) &= \frac{1}{2^n - 1} \sum_{d|2^n-1} 2^d \mu(\frac{2^n - 1}{d}) = \frac{1}{2^n - 1}[-2 + 2^{2^n-1}] \\ &= \frac{\Phi(2^{2^n-1} - 1)}{2^n - 1} = N_P(k). \end{aligned}$$

8.2 Exerciţii rezolvate

Exerciţiul 8.2.1 *O secvenţă determinată de polinomul de feedback* $1+X^3+X^4$ *are perioadă maximă?*

Rezolvare: Notăm cu $\alpha = X \bmod f(X)$ o rădacină a polinomului de feedback: $1 + \alpha^3 + \alpha^4 = 0$. Succesiv obţinem puterile lui α:
$\alpha^1=\alpha$;
$\alpha^2=\alpha^2$;
$\alpha^3=\alpha^3$;
$\alpha^4=1 + \alpha^3$;
$\alpha^5=\alpha\alpha^4 = \alpha(1 + \alpha^3) = 1 + \alpha + \alpha^3$;
$\alpha^6=\alpha\alpha^5 = \alpha(1 + \alpha + \alpha^3) = 1 + \alpha + \alpha^2 + \alpha^3$;
$\alpha^7=\alpha\alpha^6 = \alpha(1 + \alpha + \alpha^2 + \alpha^3) = 1 + \alpha + \alpha^2$;
$\alpha^8=\alpha\alpha^7 = \alpha(1 + \alpha + \alpha^2) = \alpha + \alpha^2 + \alpha^3$;
$\alpha^9=\alpha\alpha^8 = \alpha(\alpha + \alpha^2 + \alpha^3) = 1 + \alpha^2$;
$\alpha^{10}=\alpha\alpha^9 = \alpha(1 + \alpha^2) = \alpha + \alpha^3$;
$\alpha^{11}=\alpha\alpha^{10} = \alpha(\alpha + \alpha^3) = 1 + \alpha^2 + \alpha^3$;
$\alpha^{12}=\alpha\alpha^{11} = \alpha(1 + \alpha^2 + \alpha^3) = 1 + \alpha$;
$\alpha^{13}=\alpha\alpha^{12} = \alpha(1 + \alpha) = \alpha + \alpha^2$;
$\alpha^{14}=\alpha\alpha^{13} = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$;
$\alpha^{15}=\alpha\alpha^{14} = \alpha(\alpha^2 + \alpha^3) = 1$.
Ordinul lui α este $2^4 - 1$, în concluzie, polinomul de feedback este primitiv.

8.3 Exerciţii propuse

Exerciţiul 8.3.1 *O secvenţă determinată de polinomul de feedback* $1+X^2+X^4$ *are perioadă maximă?*

Răspuns: Nu. Polinomul nu este ireductibil, deci nu este primitiv.

Capitolul 9

Calcule în corpuri Galois

9.1 Breviar teoretic

Corpul Galois $GF(2^n)$ este definit de un polinom $f(X) \in Z_2[X]$ de grad n. Elementele acestui corp sunt polinoame.

Operaţiile între două polinoame $a(X) = a_0 + a_1X + \ldots a_nX^n$ şi $b(X) = b_0 + b_1X + \ldots b_nX^n$ din $GF(2^n)$ se definesc în modul următor:

a) $a(X) \oplus b(X) = c(X)$, $c_i = (a_i + b_i) \bmod 2$;

b) $a(X) \bullet b(X) = a(X)b(X) \bmod f(X)$.

Un element din $GF(2^n)$ se poate reprezenta sub forma binară (şi apoi hexazecimală) prin coeficienţii săi : $a_0 + a_1X + \ldots + a_nX^n$ se identifică cu $a_n \ldots a_1a_0$, $a_i \in \{0, 1\}$

Inversul unui element din $GF(2^n)$ se determină cu algoritmul lui Euclid, exemplificat în continuare.

9.2 Exerciţii rezolvate

Exerciţiul 9.2.1 *Care este inversul elementului* $\{45\}$ *(reprezentat în format hexa) din* $GF(2^8)$ *definit de polinomul* $f(X) = 1 + X + X^3 + X^4 + X^8$.

Rezolvare: Elementului $\{45\}$ îi corespunde polinomul $X^6 + X^2 + 1$. Pentru a afla inversul lui $\{45\} \bmod f(X)$ utilizăm algoritmul lui Euclid:

$X^8 + X^4 + X^3 + X + 1 = X^2(X^6 + X^2 + 1) + X^3 + X^2 + X + 1$,

$X^6 + X^2 + 1 = (X^3 + X^2)(X^3 + X^2 + X + 1) + 1$,

plecând de la ultima ecuaţie către prima, succesiv obţinem:

$1 = (X^3 + X^2)(X^3 + X^2 + X + 1) + X^6 + X^2 + 1$

$1 = (X^3 + X^2)(X^2(X^6 + X^2 + 1) + X^8 + X^4 + X^3 + X + 1) + X^6 + X^2 + 1$

$1 = (X^5 + X^4 + 1)(X^6 + X^2 + 1) + (X^3 + X^2 + 1)(X^8 + X^4 + X^3 + X + 1)$

deci inversul polinomului $X^6 + X^2 + 1$ este $X^5 + X^4 + 1$. Utilizând codificarea hexa ajungem la concluzia că inversul elementului $\{45\}$ este $\{31\}$.

Exerciţiul 9.2.2 *Să se adune elementele* $\{57\}$ *şi* $\{83\}$ *în corpul Galois* $GF(2^8)$ *definit de polinomul* $1 + X + X^3 + X^4 + X^8$.

Rezolvare: Scrierea binară a celor două elemente este $\{57\} = \{01010111\}$ respectiv $\{83\} = \{10000011\}$. Efectuând calculele obţinem $\{57\} \oplus \{83\} = \{11010100\} = \{D4\}$.

Exerciţiul 9.2.3 *Să se înmulţească elementele* $\{57\}$ *şi* $\{83\}$ *în corpul Galois* $GF(2^8)$ *definit de polinomul* $1 + X + X^3 + X^4 + X^8$.

Rezolvare: $\{57\} \bullet \{83\} = (X^6 + X^4 + X^2 + X + 1)(X^7 + X + 1) = X^{13} + X^{11} + X^9 + X^8 + X^6 + X^5 + X^4 + X^3 + 1 \bmod (X^8 + X^4 + X^3 + X + 1) = X^7 + X^6 + 1 = \{11000001\} = \{C1\}$.

9.3 Exerciţii propuse

Exerciţiul 9.3.1 *Care este inversul elementului* $\{33\}$ *(reprezentat în format hexa) din* $GF(2^8)$ *definit de polinomul* $1 + X + X^3 + X^4 + X^8$.

Răspuns: $\{6C\}$.

Exerciţiul 9.3.2 *Arătaţi că elementele* $\{12\}$ *şi* $\{AA\}$ *(reprezentate în format hexa) sunt inverse în corpul Galois* $GF(2^8)$ *definit de polinomul* $1 + X + X^3 + X^4 + X^8$.

Exerciţiul 9.3.3 *Să se adune elementele* $\{5\}$ *şi* $\{7\}$ *în corpul Galois* $GF(2^4)$ *definit de polinomul* $1 + X + X^4$.

Răspuns: $\{2\}$.

Exerciţiul 9.3.4 *Să se înmulţească elementele* $\{5\}$ *şi* $\{7\}$ *în corpul Galois* $GF(2^4)$ *definit de polinomul* $1 + X + X^4$.

Răspuns: $\{8\}$.

Exerciţiul 9.3.5 *Se consideră transformarea dată de*

$$g(\mathbf{y}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \mathbf{y}^{-1} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{9.1}$$

unde $\mathbf{y}^{-1}$ *este inversul lui* $\mathbf{y}$ *în corpul Galois* $GF(2^8)$ *definit de polinomul* $1 + X + X^3 + X^4 + X^8$. *Calculaţi* $g(1), g(2), g(3), g(4), g(5)$.

Răspuns: Transformarea indicată în problemă defineşte tabela de substituţie a algoritmului RIJNDAEL. Valorile solicitate (în zecimal) sunt: $g(1) = 124, g(2) = 119, g(3) = 123, g(4) = 242, g(5) = 107$.

Capitolul 10

Algoritmul RIJNDAEL - Standardul AES

10.1 Breviar teoretic

Pentru rezolvarea următoarelor exerciţii plecăm de la ipoteza cunoaşterii standardului FIPS 197 - Advanced Encryption Standard compus din patru operaţii (sumare modulo 2 cu cheia de rundă, subtituţia la nivel de octet, shiftarea liniilor, mixarea coloanelor etc.) în cadrul procesului de transformare a stărilor şi din generatorul de chei de rundă.

10.2 Exerciţii rezolvate

Exerciţiul 10.2.1 *Intrarea în runda $i = 6$ a algoritmului AES 128/128 pentru cifrarea textului ,,zero peste tot", cu ajutorul cheii ,,zero peste tot", este:*

$$\begin{bmatrix} D4 & 55 & 7E & 79 \\ 6F & B8 & 05 & 79 \\ 4F & 96 & BB & DE \\ 6C & 33 & 3D & 23 \end{bmatrix}$$

cheia de rundă fiind:

$$\begin{bmatrix} EC & 14 & 99 & 6A \\ 61 & 25 & FF & B4 \\ 4B & 75 & 09 & 9B \\ 85 & 8C & 37 & A7 \end{bmatrix}$$

Care este ieşirea după procesarea rutinelor SubBytes, ShiftRows, MixColumns şi AddRoundKey?

Rezolvare:
Rutina SubBytes presupune folosirea următorului Sbox:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Găsirea octetului din S-box corespunzator octetului din stare se face astfel: pentru octetul $D4$ se caută în SBox elementul aflat la intersecţia liniei D cu coloana 4 şi se substituie în stare elementul găsit in Sbox. $D4$ se va substitui cu 48. Procedeul se aplică similar pentru ceilalţi octeţi din stare.

Rezultatul aplicării rutinei SubBytes se constituie în următoarea stare:

$$\begin{bmatrix} 48 & FC & F3 & B6 \\ A8 & 6C & 6B & B6 \\ 84 & 90 & EA & 1D \\ 50 & C3 & 27 & 26 \end{bmatrix}$$

Rutina ShiftRows acţioneaza în felul următor asupra stării: prima linie rămane neschimbată, a doua linie se roteşte la stânga cu un octet, a treia linie se roteşte la stânga cu doi octeţi iar a patra linie se roteşte la stânga cu trei octeţi.

După aplicarea rutinei ShiftRows, starea va fi următoarea:

$$\begin{bmatrix} 48 & FC & F3 & B6 \\ 6C & 6B & B6 & A8 \\ EA & 1D & 84 & 90 \\ 26 & 50 & C3 & 27 \end{bmatrix}$$

Rutina MixColumns presupune înmulţirea fiecărei coloane din stare cu următoarea matrice fixată:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Operaţiile care rezultă din înmulţirea matricilor se fac în corpul Galois GF(2^8) şi sunt înmulţiri de polinoame modulo polinomul generator al corpului GF(2^8) care este $h(X) = X^8 + X^4 + X^3 + X + 1$. Observăm că singurele înmulţiri care apar sunt cele cu 02 şi 03. Inmulţirea cu polinomul 02 in $GF(2^8)$ înseamnă înmulţirea cu polinomul X.

Fie $f(X) = b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0$ un polinom din $GF(2^8)$. Să vedem ce presupune înmulţirea $02 * f(X)$ adică $X * f(X)$:

$$X * f(X) = b_7X^8 + b_6X^7 + b_5X^6 + b_4X^5 + b_3X^4 + b_2X^3 + b_1X^2 + b_0X(\mathrm{mod}m(X)),$$

unde $m(X)$ este polinomul generator $m(X) = X^4 + X^3 + X + 1$ al corpului Galois GF(2^8). Dacă $b_7 = 0$, atunci polinomul este în forma redusă în $GF(2^8)$ (are gradul 7).

Dacă $b_7 = 1$, atunci:

$$X * f(X) = X^8 \bmod m(X) + b_6X^7 + b_5X^6 + b_4X^5 + b_3X^4 + b_2X^3 + b_1X^2 + b_0X.$$

Deci:

$$X * f(X) = (X^4 + X^3 + X + 1) + b_6X^7 + b_5X^6 + b_4X^5 + b_3X^4 + b_2X^3 + b_1X^2 + b_0X.$$

Prin urmare, înmulţirea cu polinomul X poate fi implementată, în cazul în care bitul cel mai semnificativ al polinomului $f(X)$ este 1, ca o operaţie de shift la stânga cu 1 bit urmată de un XOR cu (00011011), care reprezintă polinomul $(X^4 + X^3 + X + 1)$.

Dacă bitul cel mai semnificativ al polinomului $f(X)$ este 0, atunci înmulţirea presupune doar operaţie de shift la stânga cu un bit.

Pentru a trece starea curentă prin rutina MixColumns, se înmulţeste pe rând fiecare coloană din stare cu matricea fixată de mai sus.

Vom prezenta doar modul de efectuare al înmulţirii:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 48 \\ 6C \\ EA \\ 26 \end{bmatrix}$$

Coloana rezultat va conţine următoarele linii:

$$\begin{bmatrix} 02 * 48 \oplus 03 * 6C \oplus EA \oplus 26 \\ 01 * 48 \oplus 02 * 6C \oplus 03 * EA \oplus 26 \\ 48 \oplus 6C \oplus 02 * EA \oplus 03 * 26 \\ 03 * 48 \oplus 6C \oplus EA \oplus 02 * 26 \end{bmatrix}$$

Rămân de efectuat înmulţirile care apar pe fiecare linie:
$02 * 48 = 02 * 01001000 = 10010000$.
$03 * 48 = 02 * 48 \oplus 48 = 11011000$.
$03 * 6C = 03 * 01101100 = 02 * 01101100 \oplus 01101100 = 11011000 \oplus 01101100 = 10110100$.
$02 * EA = 02 * 11101010 = 11010100 \oplus 00011011 = 11110001$.
$03 * EA = 02 * EA \oplus EA = 11110001 \oplus 11101010 = 00011011$.
$02 * 26 = 02 * 00100110 = 01001100$.
$03 * 26 = 02 * 26 \oplus 26 = 01001100 \oplus 00100110 = 01101010$.
După calculele rămase, coloana rezultat va fi:

$$\begin{bmatrix} E8 \\ 93 \\ 81 \\ 12 \end{bmatrix}$$

Pentru celelalte coloane din stare se procedează similar.
Starea rezultată după aplicarea rutinei MixColumns este următoarea:

$$\begin{bmatrix} E8 & 13 & 7B & 23 \\ 93 & 5D & D0 & 71 \\ 81 & 5D & 08 & 4C \\ 12 & C9 & A1 & B7 \end{bmatrix}$$

Aplicarea rutinei AddRoundKey presupune o simplă operaţie de XOR pe fiecare octet din stare cu octet-ul corespunzător din cheia de rundă.

$$\begin{bmatrix} E8 & 13 & 7B & 23 \\ 93 & 5D & D0 & 71 \\ 81 & 5D & 08 & 4C \\ 12 & C9 & A1 & B7 \end{bmatrix} \oplus \begin{bmatrix} EC & 14 & 99 & 6A \\ 61 & 25 & FF & B4 \\ 4B & 75 & 09 & 9B \\ 85 & 8C & 37 & A7 \end{bmatrix} = \begin{bmatrix} 04 & 07 & E2 & 49 \\ F2 & 78 & 2F & C5 \\ CA & 28 & 01 & D7 \\ 97 & 45 & 96 & 10 \end{bmatrix}$$

10.3 Exerciţii propuse

Exerciţiul 10.3.1 *Intrarea în runda $i = 7$ a algoritmului AES 128/128 pentru cifrarea textului ,,zero peste tot", cu ajutorul cheii ,,zero peste tot", este:*

$$\begin{bmatrix} 04 & 07 & E2 & 49 \\ F2 & 78 & 2F & C5 \\ CA & 28 & 01 & D7 \\ 97 & 45 & 96 & 10 \end{bmatrix}$$

cheia de rundă fiind:

$$\begin{bmatrix} 21 & 35 & AC & C6 \\ 75 & 50 & AF & 1B \\ 17 & 62 & 6B & F0 \\ 87 & 0B & 3C & 9B \end{bmatrix}$$

Care este ieşirea după procesarea rutinelor SubBytes, ShiftRows, MixColumns şi AddRoundKey?

Răspuns: Ieşirea din runda 7 este:

$$\begin{bmatrix} \text{B7} & \text{1D} & \text{6C} & \text{94} \\ \text{AA} & \text{25} & \text{92} & \text{E5} \\ \text{E4} & \text{2D} & \text{0F} & \text{81} \\ \text{C5} & \text{4F} & \text{81} & \text{50} \end{bmatrix}$$

Capitolul 11

Criptanaliza cifrurilor bloc

11.1 Breviar teoretic

Deoarece nu există o formulă matematică universală care să poată fi aplicată în operaţia de criptanaliză, am propus ca exerciţii la acest capitol modificări ale unor algoritmi de cifruri bloc consacrate. Sunt date o serie de indicaţii precedate de o scurtă descriere a algoritmilor propriu-zişi.

11.2 Exerciţii rezolvate

Exerciţiul 11.2.1 *Studiaţi următorele simplificări ale algoritmului RC5:*
-RC5 cu 8 *iteraţii dar fără rotaţii;*
-RC5 cu 8 *iteraţii iar numărul de rotaţii egal cu numărul de iteraţii.*

Răspuns. În cele ce urmează facem o scurtă descriere a cifrului RC5 cu r iteraţii. Acesta are lungimea blocului de date variabilă dar vom considera în cele ce urmează că aceasta a fost setată la 64 biţi. Operaţia de cifrare foloseşte $2r + 2$ chei dependente de cuvintele pe 32 biţi $S_0, S_1, S_2, \ldots, S_{2r+2}$ unde r este numărul de iteraţii. Pentru cifrare blocul de date se împarte în două părţi de 32 biţi notate cu L respectiv R (RC5 face apel la codificarea *little-endian* pentru împachetarea octeţilor în cuvinte: primul octet se transformă în cele mai puţin semnificative poziţii ale lui L, etc.). Apoi avem:

$$\begin{cases} L = L + S_0, \\ R = R + S_1. \end{cases}$$

Pentru $i = 1, \ldots, r$ se execută:

$$\begin{cases} L = ((L \oplus R) << R) + S_{2i}, \\ R = ((R \oplus L) << L) + S_{2i+1}. \end{cases}$$

Ieşirea constă în registrele L şi R. Simbolul $\oplus$ are semnificaţia sumei $\bmod 2$, simbolul $<<$ semnifică rotire circulară şi în fine simbolul $+$ are semnificaţia sumei $\bmod 2^{32}$. Operaţia de

decriptare este similară (intervin operatorii $\oplus, >>$ şi $-$). Modul de construcţie al secvenţei S (care derivă din cheie) nu este esenţial în cadrul acestui exerciţiu.

Dacă setăm numărul de iteraţii $r = 8$ şi nu facem nici un fel de rotaţii atunci pentru $i = 1, \ldots, 8$ se execută:

$$\begin{cases} L = (L \oplus R) + S_{2i}, \\ R = (R \oplus L) + S_{2i+1}. \end{cases}$$

Algoritmul astfel setat nu îndeplineşte criteriul de avalanşă strictă (schimbarea unui bit în blocul de text clar produce, în medie, schimbări de 50% la ieşire). Schema de mai sus permite atacul cu ajutorul tehnicii criptanalizei liniare pentru aflarea lui S, deci a cheii efective.

Dacă setăm numărul de iteraţii $r = 8$ şi numărul de rotaţii egal cu r atunci pentru $i = 1, \ldots, 8$ se execută:

$$\begin{cases} L = ((L \oplus R) << 8) + S_{2i}, \\ R = ((R \oplus L) << 8) + S_{2i+1}. \end{cases}$$

Algoritmul astfel setat nu îndeplineşte criteriul de avalanşă strictă. Schema de mai sus permite atacul cu ajutorul tehnicii criptanalizei diferenţial/liniare pentru aflarea lui S.

Exerciţiul 11.2.2 *Studiaţi următorele simplificări ale algoritmului DES:*
-DES cu 12 *iteraţii dar fără aplicaţiile S;*
-DES cu 4 *iteraţii;*
-DES cu 6 *iteraţii.*

Răspuns. Cifrul bloc DES (proiectat în 1977) este sub controlul unei chei efective de 56 biţi (cheia de bază este de 64 biţi, 8 biţi fiind pentru detecţia erorilor) iar mărimea blocului de date este de 64 biţi. Textul clar este permutat iar apoi este împărţit în două blocuri L şi R de lungime 32 biţi. Se execută apoi iterativ operaţiile (pentru $i = 1, \ldots,$ *numărul de iteratii*):

$$\begin{cases} L_i = R_i, \\ R_i = L_i \oplus f(R_{i-1}, K_i). \end{cases}$$

În final textul este supus permutării inverse. Ne concentrăm asupra descrierii funcţiei $f : \mathbf{Z}_2^{32} \times \mathbf{Z}_2^{48} \to \mathbf{Z}_2^{32}$. Iniţial blocul R (32 biţi) este extins cu ajutorul funcţiei E la un bloc pe 48 biţi care este sumat mod2 cu cheia K (extinsă la 48 biţi cu ajutorul algoritmului de producere a subcheilor). Opt aplicaţii $S : \mathbf{Z}_2^6 \to \mathbf{Z}_2^4$ produc o ieşire pe 32 biţi care este permutată pentru a produce ieşirea finală dintr-o iteraţie. Dacă aplicaţiile S sunt fixe (se selectează 4 biţi din 6 în mod fix) atunci se poate aplica tehnica criptanalizei diferenţiale (biţii de la ieşire sunt biţii de la intrare (sumaţi mod2 cu cheia K) dar într-o altă ordine).

Algoritmul DES cu 4 cât şi cu 6 iteraţii poate fi spart cu ajutorul tehnicii atacului cu text clar cunoscut.

11.3 Exerciţii propuse

Exerciţiul 11.3.1 *Ce defect are un algoritm de cifrare care este închis (un algoritm de cifrare se numeşte închis dacă pentru orice chei k_1 şi k_2 există o cheie k_3 astfel încât pentru orice text clar M avem $E_{k_1}E_{k_2}(M) = E_{k_3}(M)$)?*

Răspuns. Ca metodă de atac generică se poate opta pentru cifrarea repetitivă.

Exerciţiul 11.3.2 *Având la dispoziţie un cifru bloc $E_k(.)$ proiectaţi un cifru flux şi viceversa.*

Exerciţiul 11.3.3 *Scrieţi funcţia analitică a celor opt funcţii de substituţie S ale cifrului DES.*

Exerciţiul 11.3.4 *Fie $E(\cdot,\cdot)$ o funcţie de cifrare pe m biţi de cheie şi n biţi de date. Care este valoarea maximă a lui m astfel încât cheia efectivă a cifrului să fie m?*

Capitolul 12

Lema chinezească a resturilor

12.1 Breviar teoretic

Teorema 12.1 *(Lema chinezească a resturilor- CRT) Fie $m_1, \ldots, m_k$ numere întregi cu $(m_i, m_j) = 1$ pentru orice $i \neq j$. Atunci sistemul*

$$x \equiv a_i \bmod m_i$$

are o soluţie unică modulo $\prod_{i=1}^{k} m_i$.

Demonstraţie. Existenţa soluţiei. Vom nota

$$M = \prod_{i=1}^{k} m_i$$

şi

$$M_i = \frac{M}{m_i} \text{ pentru orice } i = 1, \ldots, k.$$

Deoarece $(m_i, m_j) = 1$ pentru orice $i \neq j$ avem $(M_j, m_j) = 1$ pentru orice j adică există N_j astfel ca $M_j N_j = 1 \bmod m_j$. Atunci dacă notăm

$$x = \sum_{i=0}^{k} a_i M_i N_i$$

şi reducem modulo m_i avem:

$$x = \sum_{j=0}^{k} a_j M_j N_j \bmod m_i \text{ pentru orice } i.$$

Folosind faptul că $(M_i, m_j) \neq 1$ pentru $i \neq j$ obţinem:

$$\begin{aligned} x &= a_i M_i N_i \bmod m_i \\ &= a_i \bmod m_i \ \text{ pentru orice } \ i. \end{aligned}$$

Unicitatea soluţiei. Fie $x^{'}$ şi $x^{''}$ două soluţii atunci

$$x = x^{'} - x^{''} = 0 \bmod m_i \ \text{ pentru orice } \ i$$

deci

$$x = 0 \bmod M.$$

12.2 Exerciţii rezolvate

Exerciţiul 12.2.1 *Să se rezolve sistemul de ecuaţii:*

$$\begin{cases} x \equiv 3 \mod 13 \\ x \equiv 34 \mod 47 \\ x \equiv 2 \mod 51 \end{cases}$$

Rezolvare:
Soluţia sistemului de congruenţe este dată de formula:

$$x = \sum_{j=1}^{3} a_j M_j N_j \bmod M.$$

unde $a_1 = 3, a_2 = 34, a_3 = 2$ iar $m_1 = 13, m_2 = 47, m_3 = 51$. Se observă că m_1, m_2 şi m_3 sunt prime între ele.

Calculăm $M = 13 \cdot 47 \cdot 51 = 31161$ şi $M_1 = 47 \cdot 51 = 2397$, $M_2 = 13 \cdot 51 = 663$ si $M_3 = 13 \cdot 47 = 611$.

Mai departe trebuie calculat inversul lui M_j pentru $j = 1$, $j = 2$ şi $j = 3$.

Cu algoritmul lui Euclid extins, se calculează $N_1 = M_1^{-1} \bmod m_1 = 2397^{-1} \bmod 13 = 5^{-1} \bmod 13 = 8$.

Similar se calculează $N_2 = M_2^{-1} \bmod m_2 = 663^{-1} \bmod 47 = 5^{-1} \bmod 47 = 19$, iar

$N_3 = M_3^{-1} \bmod m_3 = 611^{-1} \bmod 51 = 50^{-1} \bmod 51 = 50$.

În acest moment, avem toate datele necesare pentru a calcula soluţia x a sistemului de congruenţe:

$x = a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 \bmod M$.

Deci $x = 3{\cdot}2397{\cdot}8{+}34{\cdot}663{\cdot}19{+}2{\cdot}611{\cdot}50 \bmod 31161 = 57528{+}428928{+}61100 \bmod 31161$ de unde $x = 17819 \bmod 31161$; se poate verifica faptul că într-adevăr aceasta este soluţia sistemului.

12.3 Exerciţii propuse

Exerciţiul 12.3.1 *Să se rezolve sistemul de ecuaţii:*

$$\begin{cases} x \equiv 1 \mod 13 \\ x \equiv 2 \mod 17 \\ x \equiv 3 \mod 11 \end{cases}$$

Răspuns: $x = 1158 \bmod 2431$.

Capitolul 13

Sistemul de cifrare Merkle-Hellman

13.1 Breviar teoretic

Algoritmul de cifrare *Merkle-Hellman* constă în codificarea mesajului ca o soluţie a unei probleme de tip rucsac pentru care ponderile $\{M_1, ..., M_n\}$ constituie cheia de cifrare, şi textului clar $\{b_1, ..., b_n\}$ îi corespunde textul cifrat $\sum_{i=1}^{n} b_i M_i$.

Definiţia 13.1 *Un şir de ponderi* $\{M_1, ..., M_n\}$ *se numeşte supercrescător dacă:*

$$M_k > \sum_{i=1}^{k-1} M_i \text{ pentru orice } k. \tag{13.1}$$

Problema rucsacului supercrescător este uşor de rezolvat folosind următoarea schemă: pentru $k = n, ..., 1$:

- dacă $M_k < S$ atunci $b_k = 1$ şi $S = S - M_k$;
- altfel $b_k = 0$.

Algoritmii de tip rucsac care nu sunt supercrescători nu sunt uşor de rezolvat şi nu există niciun algoritm rapid care să rezolve problema. Singura modalitate cunoscută de a determina dacă $b_i = 1$ constă în testarea tuturor soluţiilor. Cei mai rapizi algoritmi de testare au o complexitate exponenţială.

Algoritmul Merkle-Hellman se bazează pe această proprietate: *cheia privată* este şirul ponderilor pentru un rucsac supercrescător iar *cheia publică* este şirul ponderilor pentru un rucsac care are aceeaşi soluţie, dar nu este supercrescător. *Merkle* şi *Hellman* au găsit o metodă prin care se poate transforma o problemă a rucsacului supercrescător într-o problemă normală a rucsacului. Tehnica de conversie face apel la aritmetica modulară.

Având la dispoziţie o problemă de tip rucsac supercrescător (cheia privată) cu ponderile $\{M_1, ..., M_n\}$ atunci aceasta se transformă într-o problemă de tip rucsac normală (cheia publică) cu şirul ponderilor

$$\{mM_1 \bmod p, ..., mM_n \bmod p\},$$

unde m şi p sunt numere naturale prime între ele (acestea fac parte din cheia privată) şi $p > \sum_{i=1}^{n} M_i$.

Pentru a cifra un mesaj binar acesta se va împărţi în blocuri de lungimi egale cu cardinalul mulţimii ponderilor. Cifrarea unui bloc $b_1...b_n$ va fi numărul natural:

$$\sum_{i=1}^{n} b_i(mM_i \bmod p).$$

Pentru descifrare destinatarul mesajului cunoaşte cheia privată: ponderile originale şi valorile lui m şi p. Acesta va calcula mai întâi pe $m^{-1} \bmod p$. Se va multiplica apoi textul cifrat cu $m^{-1} \bmod p$ iar după aceea se va rezolva problema rucsacului supercrescător pentru a recupera textul original.

13.2 Exerciţii rezolvate

Exerciţiul 13.2.1 *Să se construiască cheia publică pentru algoritmul Merkle-Hellman reprezentat de cheia privată* $\{2, 3, 6, 13, 27, 52\}$*, modulul* $p = 105$ *şi multiplicatorul* $m = 31$*. Cifraţi mesajul* 101110*.*

Rezolvare:

Având la dispoziţie cheia privată $\{M_1, ..., M_n\}$, cheia publică se obţine astfel $\{mM_1 \bmod p, ..., mM_n \bmod p\}$.

Prin urmare, cheia privată pentru datele de mai sus este $\{31{\cdot}2 \bmod 105, 31{\cdot}3 \bmod 105, 31{\cdot}6 \bmod 105, 31 \cdot 13 \bmod 105, 31 \cdot 27 \bmod 105, 31 \cdot 52 \bmod 105\}$ adică $\{62, 93, 81, 88, 102, 37\}$.

Cifrarea mesajului 101110 ($(m_1, ..., m_6)$) se face după formula $\sum_{i=1}^{n} m_i(mM_i \bmod p)$, adică pe baza cheii publice. Rezultatul va fi $62 + 81 + 88 + 102$, deci mesajul cifrat este $c = 333$.

Exerciţiul 13.2.2 *Să se descifreze mesajul* $C = 4608$ *cifrat cu ajutorul algoritmului Merkle-Hellman cu următorii parametrii:* $n = 9$*, cheia privată* $\{1, 2, 5, 10, 19, 40, 98, 179, 355\}$*, modulul* $p = 1717$ *şi multiplicatorul* $m = 507$*.*

Rezolvare: Se determină $C \cdot m^{-1} \bmod 1717 = 4608 \cdot 507^{-1} \bmod 1717 = 4608 \cdot 657 \bmod 1717 = 385$.

Apoi se rezolvă problema supercrescătoare a rucsacului de dimensiune 385 : $385 = 355 + 19 + 10 + 1$. Mesajul clar va conţine 1 pe poziţiile corespunzătoare acestor ponderi, deci se obţine 100110001.

13.3 Exerciţii propuse

Exerciţiul 13.3.1 *Să se construiască cheia publică pentru algoritmul Merkle-Hellman reprezentat de cheia privată* $\{2, 3, 6, 13, 27, 52\}$*, modulul* $p = 105$ *şi multiplicatorul* $m = 31$*. Cifraţi mesajul* 011111*.*

Răspuns: Cheia publică $\{62, 93, 81, 88, 102, 37\}$, mesajul cifrat $c = 401$.

Capitolul 14

Sistemul de cifrare RSA

14.1 Breviar teoretic

Algoritmul *RSA* a fost inventat de către *Ron Rivest, Adi Shamir* şi *Leonard Adleman* şi a fost studiat în cadrul unor studii criptanalitice extinse. Securitatea RSA-ului se bazează pe dificultatea factorizării numerelor mari. Cheia publică şi cheia privată sunt funcţie de o pereche de numere prime mari (de 200 de cifre sau chiar mai mari). Factorizarea produsului a două numere prime implică recuperarea textului clar din textul cifrat, cunoscând cheia publică.

Pentru generarea a două chei (publică şi privată) se aleg aleatoriu două numere prime mari p şi q. Din raţionamente de securitate p şi q au acelaşi ordin de mărime. Se va calcula produsul $n = p \cdot q$. Se va alege apoi, aleatoriu, exponentul public (de cifrare) e astfel ca e şi $(p-1)(q-1)$ să fie relativ prime. Utilizând algoritmul extins al lui Euclid vom calcula exponentul privat (de descifrare) d astfel ca

$$ed \equiv 1 \bmod (p-1)(q-1).$$

Cu alte cuvinte

$$d \equiv e^{-1} \bmod (p-1)(q-1).$$

Remarcăm faptul că d şi n sunt relativ prime. Perechea (e, n) constituie cheia publică iar (d, p, q) este cheia privată. Cele două numere p şi q nu mai sunt necesare la cifrare/descifrare, dar nu vor fi niciodată făcute publice (cunoaşterea lor şi a exponentului de cifrare e conduce imediat la determinarea coeficientului de descifrare d, deci sistemul de criptare devine inutil).

Pentru a cifra un mesaj M îl vom diviza în blocuri de lungime mai mică n (cu date binare vom alege cea mai mare putere a lui 2 mai mică decât n). Dacă p şi q sunt numere prime de 100 cifre atunci n va avea sub 200 de cifre iar fiecare mesaj bloc M_i va avea sub 200 de cifre. Dacă trebuie cifrate blocuri de lungime fixă atunci vom apela la operaţia de padding cu zero. Mesajul cifrat C se va obţine prin concatenarea mesajelor C_i care au aproximativ aceeiaşi lungime. Formula de cifrare va fi:

$$C_i \equiv M_i^e \bmod n.$$

Pentru a descifra un mesaj se calculează:

$$M_i \equiv C_i^d \bmod n,$$

deoarece

$$\begin{aligned} C_i^d &\equiv (M_i^e)^d \equiv M_i^{ed} \equiv M_i^{k(p-1)(q-1)+1} \\ &\equiv M_i M_i^{k(p-1)(q-1)} \equiv M_i \bmod n. \end{aligned}$$

Observaţia 14.1 *Pentru a evita metodele de factorizare cunoscute numerele p şi q trebuie să fie numere prime tari. Un număr prim p se numeşte număr prim tare dacă:*
i) $p-1$ are un factor mare r;
ii) $p+1$ are un factor mare s;
iii) $r-1$ are un factor mare t.

Operaţia de semnare a unui mesaj M se realizează prin exponenţierea amprentei $H(M)$ cu ajutorul cheii private: $s = H(M)^d \bmod n$. Verificarea semnăturii se realizează prin comparaţia lui $H(M)$ cu $s^e \bmod n$.

În cazurile practice valoarea lui e este un număr relativ mic, deci d are o valoare mare. Acest lucru conduce la timpi de rulare diferiţi între operaţiile private (descifrare/semnare) şi cele publice(cifrare/verificare semnătură).

Pentru optimizarea calculelor de verificare a semnăturii se poate utiliza lema chinezească a resturilor (CRT), însă acest lucru induce vulnerabilităţi în mediul de implementare.

Astfel, dacă $p > q$, sunt **precalculate** valorile:

$$\begin{aligned} dP &= (e^{-1} \bmod n) \bmod (p-1), \\ dQ &= (e^{-1} \bmod n) \bmod (q-1), \\ qInv &= q^{-1} \bmod p. \end{aligned}$$

În **faza de calcul** se execută:

$$\begin{aligned} m_1 &= c^{dP} \bmod p, \\ m_2 &= c^{dQ} \bmod q, \\ h &= qInv(m_1 - m_2) \bmod p, \\ m &= m_2 + hq. \end{aligned}$$

Cheia privată ce se stochează fiind $(p, q, dP, dQ, qInv)$.

14.2 Exerciţii rezolvate

Exerciţiul 14.2.1 *Se dă numărul $n = 36187829$ despre care se cunoaste faptul că este un produs de două numere cu valoarea $\phi(n) = 36175776$. Factorizaţi numărul n.*

Rezolvare: Folosim relaţile $p + q = n - (p - 1)(q - 1) + 1$ şi $p - q = \sqrt{(p+q)^2 - 4n}$. Obţinem $p = 5657$ şi $q = 6397$.

Exerciţiul 14.2.2 *Să se cifreze mesajul $M = 3$, utilizând sistemul RSA cu următorii parametrii: $N = 187$ (modulul de cifrare), $e = 7$ (exponentul de cifrare).*

Rezolvare: Criptograma este: $C = M^e = 3^7 = 2187 = 130 \bmod 187$.

Exerciţiul 14.2.3 *Să se descifreze mesajul $C = 130$, utilizând sistemul RSA cu următorii parametrii: $N = 187 = 11 \cdot 17$ (modulul de cifrare), $e = 7$ (exponentul de cifrare).*

Rezolvare: Deoarece se cunoaşte factorizarea $N = 11 \cdot 17$, se poate calcula $\varphi(N) = 16 \cdot 10 = 160$, $\varphi(\varphi(N)) = 64$.

Exponentul de descifrare va fi:

$d = e^{\varphi(\varphi(N))-1} = 7^{63} = (7^9)^7 = (40353607)^7 = 7^7 = 823543 = 23 \bmod 160$.

Descifrarea mesajului cifrat C va fi: $C^d = 130^{23} = 3 = M \bmod 187$.

Exerciţiul 14.2.4 *Să se descifreze, utilizând CRT, mesajul cifrat $c = 8363$, pentru cazul în care $p = 137$, $q = 131$, $n = p \cdot q = 17947$, $e = 3$, $d = 11787$.*

Rezolvare: În faza de precalcul avem:

$$\begin{aligned} dP &= (e^{-1} \bmod n) \bmod (p-1) = 91, \\ dQ &= (e^{-1} \bmod n) \bmod (q-1) = 87, \\ qInv &= q^{-1} \bmod p = 114. \end{aligned}$$

Calculăm apoi:

$$\begin{aligned} m_1 &= c^{dP} \bmod p = 102, \\ m_2 &= c^{dQ} \bmod q = 120, \\ h &= qInv(m_1 - m_2) \bmod p = 3, \\ m &= m_2 + hq = 513. \end{aligned}$$

14.3 Exerciţii propuse

Exerciţiul 14.3.1 *Fie numerele prime $p = 211$ şi $q = 167$. Să se cifreze mesajul TEST cu ajutorul algoritmului RSA, utilizând exponentul public $e = 2^8 + 1$. Elementele din mesajul clar se codifică conform codului ASCII.*

Răspuns: $N = 35237$, $\phi(N) = 34860$, $d = 23873$, mesajul cifrat este: 01154 05746 04357 01154.

Exerciţiul 14.3.2 *Să se descifreze mesajul 01154 05746 04357 01154 cu ajutorul algoritmului RSA ($p = 211$ şi $q = 167$), utilizând exponentul public $e = 2^8 + 1$. Elementele din mesajul clar se decodifică conform codului ASCII.*

Răspuns: $N = 35237$, $\phi(N) = 34860$, $d = 23873$, mesajul clar este TEST.

Capitolul 15

Sistemul de cifrare ElGamal

15.1 Breviar teoretic

Algoritmul de cifrare ElGamal este definit de un număr prim p şi un element $g \in Z_p^*$ primitiv, numit generator. Pentru cheia privată $x \in Z_p^*$ se calculează $y = g^x \bmod p$, cheia publică fiind tripletul (y, g, p).

Pentru a cifra un mesaj $M \in Z_p$ se alege aleatoriu $k \in Z_{p-1}$, textul cifrat fiind $(y_1, y_2) = (g^k \bmod p, My^k \bmod p)$.

Pentru a descifra mesajul (y_1, y_2) se calculează $y_2(y_1^x)^{-1} \bmod p$.

15.2 Exerciţii rezolvate

Exerciţiul 15.2.1 *Să se cifreze mesajul $M = 4$ cu ajutorul algoritmului ElGamal cu parametrii $p = 17$, $g = 14$, $x = 2$.*

Rezolvare: Cheia publică este $(y, g, p) = (14^2 \bmod 17, 14, 17) = (9, 14, 17)$, cheia privată $x = 2$. Alegem, spre exemplu, $k = 7$ relativ prim cu $16 = p - 1$. Obţinem mesajul cifrat $C = (14^7 \bmod 17, 4 \cdot 9^7 \bmod 17) = \{6, 8\}$.

Exerciţiul 15.2.2 *Să se descifreze mesajul $\{6, 8\}$, ştiind că a fost cifrat cu ajutorul algoritmului ElGamal cu parametrii $p = 17$, $g = 14$, $x = 2$.*

Rezolvare: Cheia publică este $\{y, g, p\} = \{9, 14, 17\}$, cheia privată $x = 2$. Mesajul clar se obţine aplicând formula $y_2 y_1^{-x} \bmod p = 4$.

15.3 Exerciţii propuse

Exerciţiul 15.3.1 *Să se cifreze mesajul 5 cu ajutorul algoritmului ElGamal cu parametrii $p = 23$, $g = 14$, $x = 2$. Valoarea k utilizată pentru cifrare este 7.*

Răspuns: Mesajul cifrat este $(19, 11)$.

Exerciţiul 15.3.2 *Să se descifreze mesajul* $(17, 9)$ *cu ajutorul algoritmului ElGamal cu parametrii* $p = 47$, $g = 4$, $x = 2$.

Răspuns: Mesajul clar este 8.

Capitolul 16

Aritmetica pe curbe eliptice

16.1 Breviar teoretic

Definiţia 16.1 *O curbă eliptică E este constituită din elemente (numite puncte) de tipul (x, y) ce satisfac ecuaţia:*

$$y^2 \equiv x^3 + ax + b \bmod p$$

unde a şi b sunt constante astfel încât $4a^3 + 27b^2 \neq 0 \bmod p$ şi p este un număr prim, împreună cu un element singular, notat $\mathcal{O}$ şi numit punctul de la infinit. Acest punct poate fi privit ca fiind punctul din vârful şi de la baza oricărei linii verticale.

O curbă eliptică E are o structură de grup abelian împreună cu operaţia adunare. Adunarea a două puncte de pe o curbă eliptică este definită în concordanţă cu o mulţime simplă de reguli (vezi figura 16.1).

Fiind date două puncte pe E, $P_1(x_1, y_1)$ şi $P_2(x_2, y_2)$, avem următoarele cazuri:

- dacă $x_2 = x_1$ şi $y_2 = -y_1$ atunci $P_1 + P_2 = \mathcal{O}$.
- altfel $P_1 + P_2 = (x_3, y_3)$, unde:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

cu

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{ dacă } P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1}, \text{dacă } P_1 = P_2. \end{cases}$$

Observaţia 16.1 *A nu se confunda punctul la infinit $\mathcal{O}$ cu perechea $(0, 0)$. Punctul la infinit aparţine tuturor curbelor eliptice, în timp ce punctul $(0, 0)$ este un element doar pentru curbele eliptice cu parametrul $b = 0$.*

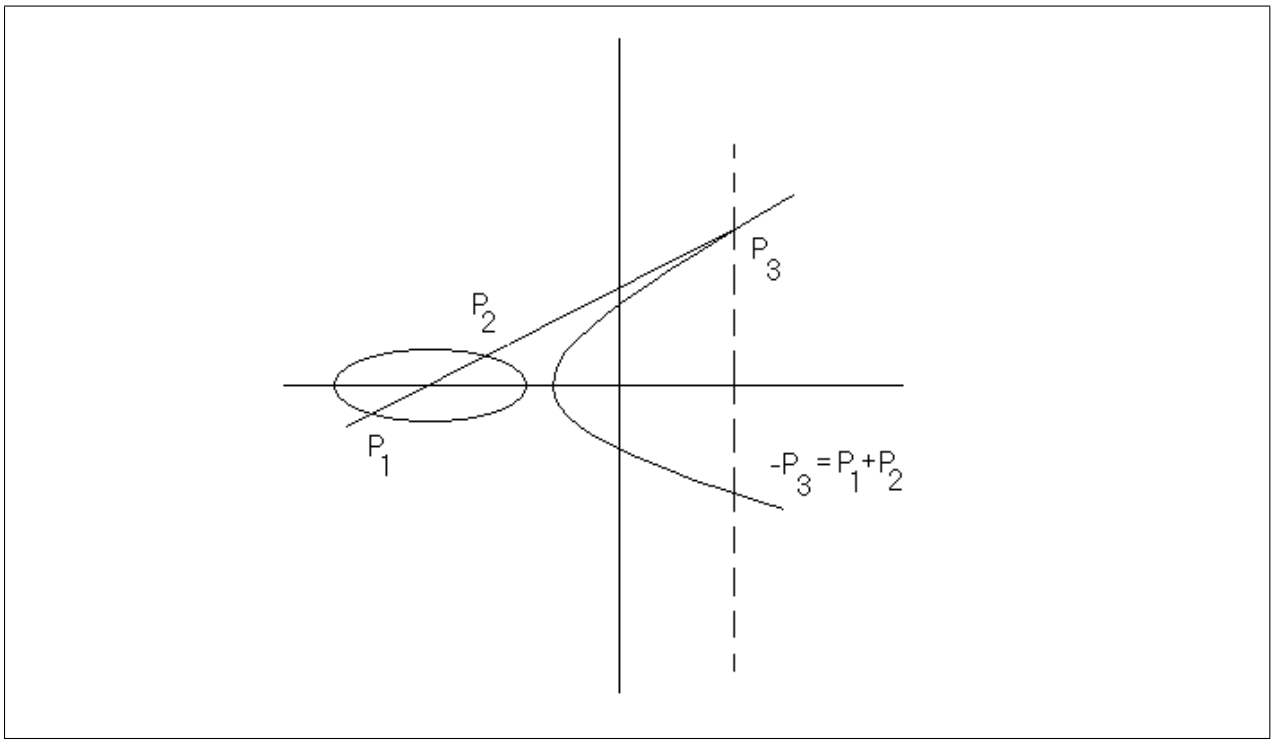

Figura 16.1: Operaţia de adunare pe o curbă eliptică.

16.2 Exerciţii rezolvate

Exerciţiul 16.2.1 *Fie curba eliptică* $y^2 = x^3+7x+4$ *definită peste* F_{71}. *Să se adune punctele* $P(15, 17)$ *şi* $Q(43, 24)$.

Rezolvare:
Coordoantele punctului $P + Q = (x_3, y_3)$, sunt date de formulele:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

unde $\lambda = \frac{y_2-y_1}{x_2-x_1}$.

Pentru calculul $\lambda = 7 \cdot (28^{-1} \bmod 71)$, se foloseşte algoritmul lui Euclid care gaseşte $33 = 28^{-1} \bmod 71$, deci $\lambda = 231$.

Atunci $x_3 = 231^2 - 15 - 43 \bmod 71 = 53$ iar $y_3 = 231(15 - 53) - 17 \bmod 71 = 9$. În concluzie, coordoantele punctului care reprezinta suma celor doua puncte de pe curba eliptică dată sunt $(53, 9)$.

Exerciţiul 16.2.2 *Fie curba eliptică* $y^2 = x^3 + x + 3$ *definită peste* F_{17}. *Arătaţi că punctul* $(2, 8)$ *este un generator al punctelor de pe curba eliptică.*

Rezolvare: Succesiv putem scrie $1P = (2, 8)$, $2P = (12, 3)$, $3P = (16, 16)$, $4P = (8, 8)$, $5P = (7, 9)$, $6P = (6, 15)$, $7P = (11, 6)$, $8P = (3, 13)$, $9P = (3, 4)$, $10P = (11, 11)$, $11P = (6, 2)$, $12P = (7, 8)$, $13P = (8, 9)$, $14P = (16, 1)$, $15P = (12, 14)$, $16P = (2, 9)$, $17P = O$.

16.3 Exerciţii propuse

Exerciţiul 16.3.1 *Fie curba eliptică* $y^2 = x^3+2x+3$ *definită peste* F_{23}. *Să se adune punctele* $P(6,1)$ *şi* $Q(13,8)$.

Răspuns: $R(5,0)$.

Exerciţiul 16.3.2 *Fie curba eliptică* $y^2 = x^3 + 6x + 11$ *definită peste* F_{17}. *Se dă punctul* $P(6,5)$. *Aflaţi* $2P$.

Răspuns: $(1,1)$.

Exerciţiul 16.3.3 *Fie curba eliptică* $y^2 = x^3 + x + 3$ *definită peste* F_7. *Arătaţi că punctul* $(4,6)$ *este un generator al punctelor de pe curba eliptică.*

Răspuns: Succesiv obţinem $1P = (4,6)$, $2P = (6,1)$, $3P = (5,0)$, $4P = (6,6)$, $5P = (4,1)$, $6P = O$.

Capitolul 17

Sistemul de cifrare ElGamal bazat pe curbe eliptice

17.1 Breviar teoretic

Algoritmul ElGamal poate fi extins pe orice grup finit $(G, \circ)$, în care problema logaritmului discret este dificilă, în particular şi pe grupul punctelor de pe o curbă eliptică.

Astfel, fie $\alpha \in G$ pentru care problema logaritmului în subgrupul $H = \{\alpha^i | i \geq 0\}$ este dificilă. Pe baza cheii private $x \in Z$, se construieşte $\beta = \alpha^x$, cheia publică fiind $\{G, \alpha, \beta\}$.

Pentru a cifra un mesaj M se alege aleatoriu $k \in Z_{|H|}$ şi se aplică regula de cifrare: $E(M, k) = (\alpha^k, M \circ \beta^k)$.

Mesajul clar m se recuperează din mesajul cifrat (y_1, y_2) după regula: $y_2 \circ (y_1^x)^{-1}$. Într-adevăr $y_2 \circ (y_1^x)^{-1} = M \circ \beta^k \circ ((\alpha^k)^x)^{-1} = M \circ \alpha^{kx} \circ (\alpha^{kx})^{-1} = M$.

17.2 Exerciţii rezolvate

Exerciţiul 17.2.1 *Să se cifreze mesajul* $(10, 9)$ *utilizând curba eliptică (publică)* $E : y^2 = x^3 + x + 6$ *pe* $\mathbf{Z}_{11}$ *cu ajutorul algoritmului ElGamal.*

Rezolvare: Pentru a calcula punctele curbei eliptice se calculează valorile $z = x^3 + x + 6 \bmod 11$, se vede care din aceste valori sunt reziduri pătratice cu ajutorul teoremei lui Euler (z este reziduu pătratic dacă şi numai dacă $z^{\frac{p-1}{2}} \equiv 1 \bmod p$) şi apoi se calculează rădăcinile pătrate ale acestor reziduri prin formula $y = \pm z^{\frac{p+1}{2}} \bmod p$). Punctele curbei eliptice vor fi: $\{(2,7), (2,4), (3,5), (3,6), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9), \mathcal{O}\}$.

Grupul E este grup ciclic (numărul de elemente este al grupului este număr prim) şi se ia ca generator pentru acesta elementul (public) $\alpha = (2, 7)$. Cheia privată de descifrare, notată prin d, este o valoare între 1 şi numărul de puncte de pe o curbă eliptică -1. Cheia publică, notată prin β, se obţine din α şi exponentul secret d prin formula $\beta = d\alpha$.

Operaţia de cifrare a mesajul M cu ajutorul cheii (secrete) k este:

$$E(M, k) = (k\alpha, M + k\beta).$$

Operaţia de descifrare pentru a obţine M este:

$$D_k(y_1, y_2) = y_2 - dy_1.$$

Fie $d = 3$. Se determină $\beta = 3(2, 7) = (8, 3)$.

Considerând valoarea aleatoare $k = 4$, se obţine: $E(M, k) = (4(2, 7), (10, 9) + 4(8, 3)) = ((10, 2), (10, 9) + (2, 4)) = ((10, 2), (3, 5))$

Exerciţiul 17.2.2 *Să se descifreze mesajul* $((10, 2), (3, 5))$ *ştiind că a fost cifrat cu algoritmul ElGamal utilizând curba eliptică(publică)* $E : y^2 = x^3 + x + 6$ *pe* $\mathbf{Z}_{11}$ *şi cheia privată* $d = 3$.

Rezolvare: Se determină mesajul clar ca fiind: $M = y_2 - dy_1 = (3, 5) - 3(10, 2) = (3, 5) - (2, 4) = (3, 5) + (2, 7) = (10, 9)$.

17.3 Exerciţii propuse

Exerciţiul 17.3.1 *Se consideră algoritmul ElGamal precizat de parametrii* $E : y^2 = x^3 + x + 6$ *peste* $\boldsymbol{Z}_{11}$. *Arătaţi că* $\alpha = (2, 7)$ *este un generator al grupului* E. *Se consideră cheia privată* $d = 5$. *Să se cifreze mesajul* $(10, 9)$ *cu valoarea aleatoare* $k = 3$.

Răspuns: Valoarea cheii publice este $\beta = d\alpha = (3, 6)$. Mesajul cifrat este $(k\alpha, M + k\beta) = ((8, 3), (10, 9) + (5, 2)) = ((8, 3), (5, 9))$.

Exerciţiul 17.3.2 *Se consideră algoritmul ElGamal precizat de parametrii* $E : y^2 = x^3 + x + 6$ *peste* $\boldsymbol{Z}_{13}$. *Arătaţi că* $\alpha = (4, 3)$ *este un generator al grupului* E. *Să se descifreze mesajul* $((9, 4), (2, 9))$ *cu ajutorul cheii private* $d = 3$.

Răspuns: $D_k(y_1, y_2) = (y_2 - dy_1) = ((2, 9) - 3(9, 4)) = ((2, 9) - (4, 10)) = ((2, 9) + (4, 3)) = (3, 7)$.

Capitolul 18

Sistemul de cifrare Menezes-Vanstone

18.1 Breviar teoretic

În acest sistem de cifrare - de fapt o variantă a lui ElGamal - curba eliptică este utilizată pentru mascare, textele clare şi cele cifrate putând fi formate din orice elemente nenule (nu neapărat puncte din E).

Fie E o curbă eliptică peste Z_p, $p > 3$ număr prim care conţine un subgrup ciclic G în care problema logaritmului discret este dificilă. Pe baza cheii private $d \in Z$, se construieşte $\beta = d\alpha$, cheia publică fiind $\{E, \alpha, \beta\}$.

Pentru a cifra mesajul $m = (m_1, m_2) \in Z_p^* \times Z_p^*$ se alege aleatoriu k şi se construieşte textul cifrat (y_0, y_1, y_2) după regulile:

$$y_0 = k\alpha,\ (c_1, c_2) = k\beta,\ y_i = c_i m_i,\ i = 1, 2.$$

La descifrare, cunoscând (y_0, y_1, y_2) şi cheia privată d se determină textul clar astfel:

$$(m_1, m_2) = (y_1 c_1^{-1} \bmod p, y_2 c_2^{-1} \bmod p), \text{ unde } dy_0 = (c_1, c_2)$$

18.2 Exerciţii rezolvate

Exerciţiul 18.2.1 *Se consideră algoritmul Menezes-Vanstone precizat de parametrii* $E : y^2 = x^3 + x + 6$ *peste* $\boldsymbol{Z}_{13}$. *Arătaţi că* $\alpha = (4, 3)$ *este un generator al grupului* E. *Se consideră cheia privată* $d = 3$. *Să se cifreze mesajul* $(3, 7)$ *cu valoarea aleatoare* $k = 4$.

Rezolvare: Curba eliptica are 13 puncte deci grupul E este ciclic şi orice element este generator.

Se calculează $\beta = 3\alpha = 3 \cdot (4, 3) = (3, 7)$

Cifrarea mesajului $(3, 7)$ cu valoarea aleatoare $k = 4$ se face dupa următoarea formulă $e_k(x, k) = (y_0, y_1, y_2)$ unde $y_0 = k \cdot \alpha, (c_1, c_2) = k \cdot \beta, y_i = c_i \cdot x_i (\mathrm{mod} p)$ pentru $i = 1, 2$.

Calculăm $y_0 = 4 \cdot (4, 3) = (9, 4)$ iar $(c_1, c_2) = 4 \cdot \beta = 12\alpha = (4, 10)$ deci $c_1 = 4$ iar $c_2 = 10$

Se calculează şi $y_1 = 4 \cdot 3 \bmod 13 = 12$ şi $y_2 = 10 \cdot 7 \bmod 13 = 5$. Rezultatul cifrarii mesajului $(3, 7)$ cu valoarea aleatoare $k = 4$ este ((9,4), 12,5).

18.3 Exerciţii propuse

Exerciţiul 18.3.1 *Se consideră algoritmul Menezes-Vanstone precizat de parametrii* $E : y^2 = x^3 + x + 6$ *peste* $\boldsymbol{Z}_{13}$. *Arătaţi că* $\alpha = (4, 3)$ *este un generator al grupului* E. *Se consideră cheia privată* $d = 3$. *Să se cifreze mesajul* $(1, 1)$ *cu valoarea aleatoare* $k = 2$.

Răspuns: $\beta = (3, 7)$, $(y_0, y_1, y_2) = ((2, 9), 11, 3)$.

Exerciţiul 18.3.2 *Se consideră algoritmul Menezes-Vanstone precizat de parametrii* $E : y^2 = x^3 + 2x + 7$ *peste* $\boldsymbol{Z}_{23}$. *Cunoscând cheia publică* $(\alpha, \beta) = ((5, 21), (16, 15))$, *să se cifreze mesajul* $(8, 10)$ *cu valoarea aleatoare* $k = 4$.

Răspuns: $(y_0, y_1, y_2) = ((21, 8), 13, 12)$.

Exerciţiul 18.3.3 *Se consideră algoritmul Menezes-Vanstone precizat de parametrii* $E : y^2 = x^3 + 5x + 4$ *peste* $\boldsymbol{Z}_{19}$. *Cunoscând cheia privată* $d = 2$, *să se descifreze mesajul* $(y_0, y_1, y_2) = ((17, 9), 12, 14)$.

Răspuns: $(m_1, m_2) = (11, 11)$.

Capitolul 19

Resurse software

19.1 CrypTool

CrypTool este un pachet software dedicat simulării şi analizei de mecanisme criptologice într-un mod ilustrativ. De la rolul iniţial de instruire în domeniul securităţii personalului diverselor companii private, CrypTool a evoluat într-un proiect educaţional de tip open source cu aplicaţii în domeniul criptografiei şi majoritatea domeniilor conexe. Produsul vizează în primul rând studenţii facultăţilor de matematică şi informatică, a firmelor ce activează în domeniul securitaţii informaţiilor precum şi a dezvoltatorilor de aplicaţii sau utlizatorilor de calculatoare în general care doresc sa-şi dobândească bagajul minimal de cunoştinţe criptografice.

În prezent produsul este gratuit şi disponibil în mai multe versiuni, prima dintre acestea fiind CrypTool 1.4.x dezvoltată integral în mediul $C++$. Aceasta s-a extins ulterior în alte două versiuni, încă aflate la nivel beta, ce folosesc standarde de dezvoltare de ultimă generaţie aflându-se într-o continuă actualizare. Astfel, în iulie 2008, s-a lansat CryptTool 2.0 dezvoltat în mediul $C\#$, versiune ce furnizează o paleta mai largă de funcţionalităţi combinată cu o interfaţă grafică cu facilităţi de tip "drag-and-drop". La începutul lui 2010 s-a lansat versiunea JCrypTool dezvoltată în mediul Java, avantajele acestei versiuni fiind că este independentă de platforma pe care rulează (Windows, Linux, Mac) şi că foloşeşte din plin puternicul instrument FlexiProvider prin care se pot încărca cu uşurinţă module criptografice în orice aplicaţie construită peste JCA (Java Cryptography Architecture).

CrypTool a fost dezvoltat în colaborare cu instituţii de învăţământ devenind astfel un soft educaţional şi un bun instrument de iniţiere în domeniul criptologiei, folosindu-se în prezent cu succes in multe universităţi de prestigiu. Datorită manipulării facile a mecanismelor criptologice precum şi a vizualizării şi prezentării într-o manieră facilă şi inedită a rezultatelor, CrypTool poate reprezenta componenta practică a cursurilor teoretice din domeniul criptologiei precum şi o metodă rapidă de familiarizare cu componente esenţiale ale acestui domeniu.

Produsul acoperă ambele ramuri ale criptologiei şi anume *criptografia* şi *criptanaliza*.

Sunt tratate majoritatea aspectelor fundamentale ale criptografiei. Astfel, produsul are

implementate facilităţi în cadrul fiecărui subdomeniu după cum urmează:

• criptografia clasică: cifrurile Caesar, substituţie monoalfabetică, substituţie omofonică, Vigenère, Hill, Playfair, ADFGVX, Addition, XOR, Vernam, Solitaire etc;

• criptografia simetrică modernă: cifrurile IDEA, RC2, RC4, DES, 3DES, DESX precum şi toţii finaliştii cifrului AES şi anume MARS, RC6, Rijndael, Serpent and Twofish;

• criptografia asimetrică: RSA;

• criptografia hibridă: cifrarea datelor realizâdu-se cu algoritmi simetrici (AES), protecţia cheii de cifrare fiind asigurată prin metode asimetrice (RSA);

• semnături digitale: RSA, DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), Nyberg-Rueppel;

• funcţii hash: MD2, MD4, MD5, SHA, SHA-1, SHA-2, RIPEMD-160;

• generatoare aleatoare: secude, $x^2 \bmod n$, LCG (linear congruence generator), ICG (inverse congruence generator).

În cadrul criptanalizei se regăsesc implementate majoritatea atacurilor standard după cum urmează:

• atac cu text cifrat: Caesar, Vigenère, Addition, XOR, Substitution, Playfair;

• atac cu text clar: Hill, Single-column transposition;

• atac manual: substituţie mono alfabetică, Playfair, ADFGVX, Solitaire;

• atac prin forţă brută: pentru toţi algoritmii; se presupune fie că entropia textului clar este mică sau cheia este parţial cunoscută sau alfabetului textului clar este cunoscut;

• atacuri asupra RSA: bazate pe factorizare sau tehnici care apelează la structurile algebrice (latice);

• atacuri asupra sistemelor hibride: atacuri asupra RSA sau AES(side channels attacks);

• atacuri asupra semnaturilor digitale: RSA prin factorizare; viabil până la lungime de 250 biţi (adica 75 cifre);

• atacuri asupra funcţiilor hash: generare coliziuni texte ASCII cu paradoxul zilelor de naştere (până la 40 biţi);

• analiză aleatorism: bateria de teste FIPS-PUB-140-1, periodicitate, Vitany, entropie, histograme, autocorelaţii, testul de compresie ZIP etc.

În sprijinul utilizatorilor, CrypTool are implementate o serie de demo-uri şi animaţii prin care sunt exemplificate diverse facilităţi pe care produsul le oferă folosindu-se primitive criptografice suportate şi implementate în aplicaţie ca de exemplu Caesar, Vigenère, Nihilist, DES (toate patru cu ANIMAL), Enigma (Flash), Rijdael/AES (Flash and Java), criptare hibridă şi decriptare (AES-RSA şi AES-ECC), generare şi verificare de semnături digitale, protocolul de schimb de chei Diffie-Hellman, secret sharing (CRT sau Shamir), metoda challenge-response (autentiicare), atacuri tip side-channel, securizarea e-mail-ului prin protocolul S/MIME (Java şi Flash), prezentări grafice 3D pentru date (pseudo)aleatoare, sensibilitatea funcţiilor hash privind modificări ale textului clar, teoria numerelor şi cripto sisteme RSA (Authorware).

CrypTool conţine şi un modul educaţional interactiv dedicat aplicaţiilor criptografice ce necesită aspecte elementare de teoria numerelor denumit "NT". Acest modul introduce utilizatorul în probleme elementare de teoria numerelor precum algoritmul lui Euclid pentru

găsirea celui mai mare divizor comun, testul Fermat pentru primalitate, factorizarea Fermat, factorizarea Pollard Rho şi altele.

Un alt avantaj al produslui CrypTool îl reprezintă existenţa unui meniu de documentare consistent şi o extindere online a acestuia conţinând în plus explicaţii privind noţiuni generale de criptografie, o cronologie privind dezvoltarea domeniului, exemple de utilizare a facilităţilor aplicaţiei, index sortat pe topicuri criptografice şi listă de referinţe.

Faptul că pachetul software este open source, că acoperă aspecte legate atât de criptografia clasică cât şi cea modernă, a modalităţilor multiple de simulare şi vizualizare originale, precum şi a modului facil de aplicare şi analiză a mecanismelor criptografice ne conduc la concluzia ca pachetul CrypTool reprezintă atât o modalitate rapidă de iniţiere în domeniul criptografiei cât şi un instrument de lucru puternic pentru specialişti în vederea studierii şi aplicării în acelaşi mediu a a diverse probleme concrete ce pot apărea in criptografie şi criptanaliză.

Bibliografie

[1] **A. Atanasiu**, *Securitatea Informaţiei, vol. 1, Criptografie*, ed. InfoData, Cluj, 2008.

[2] **A. Atanasiu**, *Securitatea Informaţiei, vol. 2, Protocoale de securitate*, ed. InfoData, Cluj, 2009.

[3] **T. Baignères, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay**, *A Classical Introduction to Cryptography Exercise Book*, Springer, ISBN 978-0-387-27934-3, 2006.

[4] **A.J. Menenzes**, *Handbook of Applied Cryptography*, CRC Press, 1997.

[5] **E. Simion şi Gh. Oprişan**, *Elemente de Cercetări Operaţionale şi Criptologie*, Politehnica Press, ISBN 973-8449-006, 2002.

[6] **E. Simion, V. Preda şi A. Popescu**, *Criptanaliza. Rezultate şi Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.

[7] **E. Simion**, *Enciclopedie Matematică*, Ediţie coordonată de M. Iosifescu, O. Stănăşilă şi D. Ştefănoiu, Editura AGIR, ISBN 978-973-720-288-8, pp. 905-944, 2010.

[8] **B. Schneier,** *Applied Cryptography*, Adison-Wesley, 1998.