

CRIPTOGRAFIE

Emil Simion

Cuvânt înainte

Lucrarea de față conține aplicații practice abordate de autori în cadrul seminariilor ce se desfășoară la disciplina *Criptografie și Securitate*, la Facultatea de Matematică Informatică din cadrul Universității din București, la masterul de *Securitatea Tehnologiei Informației*, organizat de Academia Tehnică Militară, precum și la masterul de *Teoria Codării și Stocării Informației*, organizat de Facultatea de Științe Aplicate din cadrul Universității Politehnica București.

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

Întrucât criptografia este o disciplină computațională, autorii au considerat utilă introducerea unui capitol special dedicat aplicațiilor software care pot constitui logistica necesară desfășurării în bune condiții a laboratoarelor la această disciplină.

În continuare considerăm util să definim unele dintre principalele noțiuni utilizate în cadrul acestui curs.

Criptologia este știința scrierilor secrete, având drept obiect apărarea secretului datelor și informațiilor confidențiale, cu ajutorul sistemelor criptografice.

Criptografia este latura defensivă a *criptologiei*, având drept obiect de activitate elaborarea (conceperea) sistemelor criptografice și 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-și îndeplinească funcția pentru care au fost concepute. Totodată criptanaliza poate analiza sistemele criptografice ale terțelor părți (prin intermediul criptogramelor realizate cu ele) astfel încât prin spargerea acestora să obțină informații utile instituției pe care o deserveste.

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

Cheia de cifrare constituie o convenție particulară, materializată, printr-un cuvânt, frază, număr, șir numeric etc. și care dirijează (reglementează) *operația de cifrare*.

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

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

Descifrarea este operația inversă cifrării și ea constă în aplicarea sistemului de cifrare cunoscut (în prezența cheii corecte) asupra criptogramelor pentru aflarea mesajului clar.

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

Dr. mat. Emil Simion

Cuprins

1	Sistemul de cifrare Cezar	1
1.1	Breviar teoretic	1
1.2	Exerciții rezolvate	1
2	Metoda substituției	3
2.1	Breviar teoretic	3
2.2	Exerciții rezolvate	4
3	Sistemul de cifrare Playfair	7
3.1	Breviar teoretic	7
3.2	Exerciții rezolvate	8
4	Sistemul de cifrare Hill	11
4.1	Breviar teoretic	11
4.2	Exerciții rezolvate	11
5	Sisteme de cifrare polialfabetice	15
5.1	Breviar teoretic	15
5.2	Exerciții rezolvate	16
6	Metoda transpoziției	19
6.1	Breviar teoretic	19
6.2	Exerciții rezolvate	19
7	Sisteme mixte	21
7.1	Breviar teoretic	21
7.2	Exerciții rezolvate	21
8	Generatoare pseudoaleatoare	25
8.1	Breviar teoretic	25
8.2	Exerciții rezolvate	27

9	Calculare în corpuri Galois	29
9.1	Breviar teoretic	29
9.2	Exerciții rezolvate	29
10	Algoritmul RIJNDAEL - Standardul AES	31
10.1	Breviar teoretic	31
10.2	Exerciții rezolvate	31
11	Criptanaliza cifrurilor bloc	35
11.1	Breviar teoretic	35
11.2	Exerciții rezolvate	35
12	Lema chinezească a resturilor	37
12.1	Breviar teoretic	37
12.2	Exerciții rezolvate	38
13	Sistemul de cifrare Merkle-Hellman	39
13.1	Breviar teoretic	39
13.2	Exerciții rezolvate	40
14	Sistemul de cifrare RSA	41
14.1	Breviar teoretic	41
14.2	Exerciții rezolvate	42
15	Sistemul de cifrare ElGamal	43
15.1	Breviar teoretic	43
15.2	Exerciții rezolvate	43
16	Aritmetica pe curbe eliptice	45
16.1	Breviar teoretic	45
16.2	Exerciții rezolvate	46
17	Sistemul de cifrare ElGamal bazat pe curbe eliptice	47
17.1	Breviar teoretic	47
17.2	Exerciții rezolvate	47
18	Sistemul de cifrare Menezes-Vanstone	49
18.1	Breviar teoretic	49
18.2	Exerciții rezolvate	49
	Bibliografie	51

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 $A-Z$ și cheia de cifrare este reprezentată de un număr întreg $k \in \{0, \dots, 25\}$.

În faza de preprocesare, delimitatorul de spațiu este ignorat sau înlocuit cu caracterul cel mai puțin 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 înlocuiește prin caracterul cod $(x + k) \bmod 26$. Pentru descifrare se utilizează regula inversă: $(x - k) \bmod 26$.

1.2 Exerciții rezolvate

Exercițiul 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, ținând cont de poziția 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 $(16 + 7) \bmod 26 = 23$, adică X;

Se continuă în mod analog pentru fiecare literă și în final se obține JYPWA VNYHM PL.

Exercițiul 1.2.2 *Să se decripteze mesajul:*

JAJSN SHWDU YTQTL DXNQJ SHJNX LTQIJ SXXXX

algoritmul utilizat fiind cifrul lui Cezar. Indicați cheia de cifrare.

Rezolvare: Se verifică, pe rând, toate cheile posibile, până când se obține un text cu sens.

În funcție de lungimea cheii, corespondența dintre literele textului clar și cele ale textului cifrat devine:

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

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

Decriptând fiecare caracter în corespondentul său clar se obține, 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 obține: EVEN IN CRYPTOLOGY SILENCE IS GOLDEN.

Capitolul 2

Metoda substituției

2.1 Breviar teoretic

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

Corespondența dintre cele două alfabete poate fi:

- aleatoare;
- pseudoaleatoare: plecând de la o parolă se construiește alfabetul cifrat.

Întrucât în cazul corespondenței aleatoare lucrurile sunt cât se poate de clare, vom prezenta pe scurt o metodă de construcție a corespondenței 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 apariției, literele din parolă;
- se scriu literele alfabetului care nu apar în parolă.

Corespondența 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 același procedeu dar cu inversa permutării σ).

În funcție de forma permutării substituția se numește:

- *directă* (alfabetul cifrat are același sens lexicografic cu alfabetul clar, sunt în total 26 astfel de substituții). Exemplu de substituție 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 substituții). Exemplu de substituție 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 substituții reciproce (dacă litera \mathcal{X} se substituie cu litera \mathcal{Y} atunci \mathcal{Y} se va substitui cu \mathcal{X}) și 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 substituția este directă dacă nu este specificat altfel.

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

Observația 2.1 *Cifrul de substituție are proprietatea de confuzie (ascunderea legăturii dintre textul clar și textul cifrat).*

2.2 Exerciții rezolvate

Exercițiul 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 corespondența 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:

Corepondența dintre alfabetul clar și 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

Corepondența dintre alfabetul clar și 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 spațiul este înlocuit cu cea mai puțin frecventă literă:

INȚCRIPTOGRAFIEȚNICIȚOȚREGULAȚNUȚESTEȚABSOLUTA.

Mesajul cifrat va fi:

OHDXC OFMGQ CZUOV DHOXO DGDCV QIKZD HIDVB MVDZY BGKIM Z.

Exercițiul 2.2.2 Să se descifreze mesajul:

DOJMD OVPGF OMATN BXXXX

algoritmul utilizat fiind o substituție simplă determinată de cuvântul cheie *PASSWORD*.

Rezolvare:

Corepondența dintre alfabetul clar și 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.

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 și mult mai sigur decât sistemele de substituție 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 puțin frecventă literă, litera I este asimilată cu litera J , și 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 dorește cifrată nu are literele pe aceeași 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 găsește pe aceeași linie cu prima litera a perechii în clar.

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

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

Observația 3.1 Dacă o digramă apare în textul clar în ordine inversă atunci același lucru se va întâmpla și în textul cifrat.

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

Observația 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 frecventă de atac a acestui tip de cifru constă în analiza frecvenței digramelor de text clar combinată cu metoda comparației patternurilor din textul cifrat cu patternuri din dicționar.

3.2 Exerciții rezolvate

Exercițiul 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 obține 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 și 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 colțurile I și S parcurs în sensul IQSP. Textul cifrat îl constituie digrama formată din colțurile care nu apar în textul clar, luate conform ordinii de parcurgere: QP.
- QI - întrucât literele sunt pe aceeași coloană se aplică regula cifrează în jos, descifrează în sus, obținându-se digrama XA (X este litera situată sub Q și A este litera situată sub I).
- NQ - întrucât literele sunt situate pe aceeași linie se aplică regula cifrează la dreapta, descifrează la stânga, obținându-se digrama QS(Q este în dreapta lui N și S este în dreapta lui Q).

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

Exercițiul 3.2.2 *Să se descifreze mesajul:*

UFRIL ERGPC RQAW

Algoritmul utilizat este cifrul lui Playfair, parola utilizată fiind CRIPTOGRAFIE.

Rezolvare: Matricea Playfair este aceeași din exercițiul anterior, fiind formată pornind de la aceeași parolă.

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

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

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

SECRET WRITING.

Capitolul 4

Sistemul de cifrare Hill

4.1 Breviar teoretic

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

În faza de preprocesare delimitatorul de spațiu este ignorat sau înlocuit cu caracterul cel mai puțin 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 înmulțirile: o prima subclasa are ca regulă de cifrare operația de înmulțire $\mathbf{C} = \mathbf{MK}$ cu descifrarea $\mathbf{M} = \mathbf{CK}^{-1}$ iar a doua subclasa folosește ca regulă de cifrare înmulțirea $\mathbf{C} = \mathbf{KM}$ având descifrarea corespunzătoare $\mathbf{M} = \mathbf{K}^{-1}\mathbf{C}$.

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

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

4.2 Exerciții rezolvate

Exercițiul 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 pozițiile corespunzătoare din alfabet (A - 0, B - 1, etc.) se obține:

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

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 obține: GLFSS MPBDT HB.

Exercițiul 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 pozițiile corespunzătoare din alfabet (A - 0, B - 1, etc.) se obține:

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

Se determină inversa matricii K mod 26 :

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

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

și

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

S-a obținut:

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

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

$$\mathbf{C} = (J \ E) = (9 \ 4).$$

Prin înmulțire cu cheia de descifrare se obține:

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

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 și regruparea literelor, se obține: HERBERT CLARK HOOVER.

Capitolul 5

Sisteme de cifrare polialfabetice

5.1 Breviar teoretic

Un sistem de cifrare de tip substituție polialfabetică este generalizarea sistemului de cifrare de substituție monoalfabetică, fiind compus dintr-un număr N de alfabete. Fiecare alfabet reprezintă o permutare (stabilită în funcție 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 ușor de identificat prin aplicarea analizei frecvențelor de apariție a literelor în secvențe decimate din textul cifrat.

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

Atacul sistemelor polialfabetice este similar cu atacul a N sisteme de substituție 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.

Ieșire: Textul clar corespunzător sistemului de cifrare polialfabetic.

Pas 1. Determină numărul de alfabete N .

Pas 2. Pentru $j = 0$ to 4 execută:

pentru $i = 1$ to $N - j$ execută:

aplică procedura de reconstrucție parțială (pe baza frecvențelor $(j + 1)$ -gramelor) a alfabetelor $i, \dots, i + j$.

Pas 3. Conform celor N alfabete reconstruiește textul clar.

Observația 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 dubleții, etc.*

5.2 Exerciții rezolvate

Exercițiul 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, ținând cont de poziția acestora în alfabet, se obține:

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

Rezultă textul cifrat: BCGXJ SKWAU EKJ.

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

Rezolvare: Aplicând descifrarea pentru fiecare caracter al textului cifrat, ținând cont de poziția acestora în alfabet, se obține:

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

Dupa gruparea literelor rezultă: THEODORE ROOSEVELT.

Capitolul 6

Metoda transpoziției

6.1 Breviar teoretic

Metoda transpoziției asigură, în cadrul sistemelor criptografice, realizarea difuziei: împrăștierea proprietăților statistice ale textului clar în textul cifrat. Spre exemplu, în cazul transpoziției coloanelor, textul clar se scrie, linie cu linie, într-o formă tabelară cu n coloane, acesta fiind recitat pe coloane în funcție 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 spațiu este ignorat sau înlocuit cu caracterul cel mai puțin frecvent din limba în care este textul clar (în limba română Q).

6.2 Exerciții rezolvate

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

CRIPTOGRAFIE

mesajul SI IN CRIPTOGRAFIE TACEREA ESTE AUR.

Rezolvare: Vom construi secvența 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 secvență cunoscută (în acest caz caracterul Q). Textul cifrat se obține citind coloanele tabelii 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 transpoziției N este mai mică decât lungimea parolei atunci se vor reține N caractere din parolă.

Capitolul 7

Sisteme mixte

7.1 Breviar teoretic

Sistemele mixte au la bază o cifrare succesivă a mesajului prin metoda substituției și apoi prin metoda transpoziției sau invers.

Atacarea sistemul de cifrare se realizează de la ultima sa componentă către prima. Remarcăm faptul că substituția simplă este comutativă cu operația de transpoziție deci se poate oricând aborda mai întâi substituția și apoi transpoziția. 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 și al transpoziției utilizate. În cazul utilizării unui sistem poligrafic (tabele de cifrare) și o transpoziție este recomandabilă o tehnică de tip backtracking.

7.2 Exerciții rezolvate

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

Rezolvare: Mai întâi textul este cifrat cu sistemul Cezar folosind cheia $k = 5$, deci corespondența 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 obține: LJT RJY WNH KNL ZWJ. Apoi, textul obținut se așează 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 și în final cea din dreapta): JJNNWLRW KZTYHLJ .

Exercițiul 7.2.2 *Să se decripteze mesajul următor:*

DKVUR UTUBK WFCVG ETGOC XWVWC

OCVPQ VUVWG FGHTQ VKUUV KKNKC

RKCPQ OQFKC EWVG

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

Rezolvare: Cum substituția și transpoziția sunt comutative, putem mai întâi decripta mesajul folosind Cezar cu cheia $k = 2$ și apoi decripta prin metoda transpoziției.

Pentru decriptarea mesajului folosind metoda Cezar cu $k = 2$, fiecare caracter se înlocuiește cu caracterul situat cu 2 poziții 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 transpoziției. Cum textul are 64 de caractere și permutarea este de lungime 3, atunci numărul de litere pe coloane este: 21, 21 și 22. Coloanele cu numai 21 de caractere sunt cele care corespund valorilor luate în ordine descrescătoare din permutarea inversă $\sigma^{-1} = (3, 2, 1)$:

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

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

Capitolul 8

Generatoare pseudoaleatoare

8.1 Breviar teoretic

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

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

$a(t) = g(a(t-1), \dots, a(t-n+1)) \oplus a(t-n)$, unde \oplus desemnează operația SAU exclusiv (XOR). Dacă funcția de feedback este liniară (se poate implementa doar folosind operația 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 locație de memorie a registrului se numește nivel, iar semnalele binare $a(0), a(1), \dots, a(n-1)$ sunt încărcate ca date inițiale. Perioada secvenței produse depinde atât de numărul de niveluri, cât și de detaliile conexiunilor de feedback. Mai exact, perioada maximă a secvenței care poate fi generată de un registru de deplasare cu feedback, având n niveluri și o funcție 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**, comunicații cu spectru distribuit etc. Funcția de feedback a unui **LFSR** are forma:

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

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

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

cu nedeterminata X . Acest polinom decide perioada și comportarea statistică a secvenței de ieșire. Pentru a preveni o secvență de ieșire trivială, trebuie ca starea „zero peste tot” să nu

fie stare inițială. 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 inițială, atunci el va genera una din secvențele 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 secvență netrivială de perioadă 15, cu cea mai bună statistică pe care o astfel de secvență 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 înseamnă 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 *funcția lui Euler*, desemnează cardinalul de numere naturale mai mici ca x și relativ prime cu x . Observăm că dacă un polinom $f(X)$ este primitiv atunci și polinomul *reciproc* lui adică $X^n f(\frac{1}{X})$ este primitiv. Se știe 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:

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

unde μ este *funcția lui Möbius* 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 și $\mu(1) = 1$.

Legătura între funcția lui Moebius și funcția 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:

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

8.2 Exerciții rezolvate

Exercițiul 8.2.1 O secvență determinată de polinomul de feedback $1 + X^3 + X^4$ are perioadă maximă?

Rezolvare: Notăm cu $\alpha = X \bmod f(X)$ o rădăcină a polinomului de feedback: $1 + \alpha^3 + \alpha^4 = 0$. Succesiv obținem 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.

Capitolul 9

Calculul 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.

Operațiile între două polinoame $a(X) = a_0 + a_1X + \dots + a_nX^n$ și $b(X) = b_0 + b_1X + \dots + b_nX^n$ 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 (și apoi hexazecimală) prin coeficienții săi : $a_0 + a_1X + \dots + a_nX^n$ se identifică cu $a_n \dots a_1 a_0$, $a_i \in \{0, 1\}$

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

9.2 Exerciții rezolvate

Exercițiul 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 ecuație către prima, succesiv obținem:

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

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

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

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 $\{31\}$.

Exercițiul 9.2.2 Să se adune elementele $\{57\}$ și $\{83\}$ 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 obținem $\{57\} \oplus \{83\} = \{11010100\} = \{D4\}$.

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

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

Capitolul 10

Algoritmul RIJNDAEL - Standardul AES

10.1 Breviar teoretic

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

10.2 Exerciții rezolvate

Exercițiul 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 ieșirea după procesarea rutinelor *SubBytes*, *ShiftRows*, *MixColumns* și *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 corespunzător octetului din stare se face astfel: pentru octetul $D4$ se caută în SBox elementul aflat la intersecția liniei D cu coloana 4 și se substituie în stare elementul găsit în Sbox. $D4$ se va substitui cu 48. Procedeeul se aplică similar pentru ceilalți octeți din stare.

Rezultatul aplicării rutinei SubBytes se constituie în următoarea stare:

48	FC	F3	B6
A8	6C	6B	B6
84	90	EA	1D
50	C3	27	26

Rutina ShiftRows acționează în felul următor asupra stării: prima linie rămâne neschimbată, a doua linie se rotește la stânga cu un octet, a treia linie se rotește la stânga cu doi octeți iar a patra linie se rotește la stânga cu trei octeți.

După aplicarea rutinei ShiftRows, starea va fi următoarea:

48	FC	F3	B6
6C	6B	B6	A8
EA	1D	84	90
26	50	C3	27

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

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

Operațiile care rezultă din înmulțirea matricilor se fac în corpul Galois $GF(2^8)$ și sunt înmulțiri 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 înmulțiri care apar sunt cele cu 02 și 03. Înmulțirea cu polinomul 02 în $GF(2^8)$ înseamnă înmulțirea 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 înmulțirea $02 * f(X)$ adică $X * f(X)$:

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

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:

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

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, înmulțirea cu polinomul X poate fi implementată, în cazul în care bitul cel mai semnificativ al polinomului $f(X)$ este 1, ca o operație 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 înmulțirea presupune doar operație de shift la stânga cu un bit.

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

Vom prezenta doar modul de efectuare al înmulțirii:

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

Coloana rezultat va conține 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 înmulțirile 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 operație de XOR pe fiecare octet din stare cu octet-ul corespunzător din cheia de rundă.

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

Capitolul 11

Criptanaliza cifrurilor bloc

11.1 Breviar teoretic

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

11.2 Exerciții rezolvate

Exercițiul 11.2.1 *Studiați următoarele simplificări ale algoritmului RC5:*

-RC5 cu 8 iterații dar fără rotații;

-RC5 cu 8 iterații iar numărul de rotații egal cu numărul de iterații.

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

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

Pentru $i = 1, \dots, r$ se execută:

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

Ieșirea constă în registrele L și R . Simbolul \oplus are semnificația sumei mod 2, simbolul \ll semnifică rotire circulară și în fine simbolul $+$ are semnificația sumei mod 2^{32} . Operația de

decriptare este similară (intervin operatorii \oplus, \gg și $-$). Modul de construcție al secvenței S (care derivă din cheie) nu este esențial în cadrul acestui exercițiu.

Dacă setăm numărul de iterații $r = 8$ și nu facem nici un fel de rotații atunci pentru $i = 1, \dots, 8$ se execută:

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

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

Dacă setăm numărul de iterații $r = 8$ și numărul de rotații egal cu r atunci pentru $i = 1, \dots, 8$ se execută:

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

Algoritmul astfel setat nu îndeplinește criteriul de avalanșă strictă. Schema de mai sus permite atacul cu ajutorul tehnicii criptanalizei diferențial/liniare pentru aflarea lui S .

Exercițiul 11.2.2 Studiați următoarele simplificări ale algoritmului DES:

- DES cu 12 iterații dar fără aplicațiile S ;
- DES cu 4 iterații;
- DES cu 6 iterații.

Răspuns. Cifrul bloc DES (proiectat în 1977) este sub controlul unei chei efective de 56 biți (cheia de bază este de 64 biți, 8 biți fiind pentru detecția erorilor) iar mărimea blocului de date este de 64 biți. Textul clar este permutat iar apoi este împărțit în două blocuri L și R de lungime 32 biți. Se execută apoi iterativ operațiile (pentru $i = 1, \dots, \text{numărul de iterații}$):

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

În final textul este supus permutării inverse. Ne concentrăm asupra descrierii funcției $f : \mathbf{Z}_2^{32} \times \mathbf{Z}_2^{48} \rightarrow \mathbf{Z}_2^{32}$. Inițial blocul R (32 biți) este extins cu ajutorul funcției E la un bloc pe 48 biți care este sumat mod2 cu cheia K (extinsă la 48 biți cu ajutorul algoritmului de producere a subcheilor). Opt aplicații $S : \mathbf{Z}_2^6 \rightarrow \mathbf{Z}_2^4$ produc o ieșire pe 32 biți care este permutată pentru a produce ieșirea finală dintr-o iterație. Dacă aplicațiile S sunt fixe (se selectează 4 biți din 6 în mod fix) atunci se poate aplica tehnica criptanalizei diferențiale (biții de la ieșire sunt biții de la intrare (sumați mod2 cu cheia K) dar într-o altă ordine).

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

Capitolul 12

Lema chinezească a resturilor

12.1 Breviar teoretic

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

$$x \equiv a_i \pmod{m_i}$$

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

Demonstrație. Existența soluției. Vom nota

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

și

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

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 $M_j N_j = 1 \pmod{m_j}$. Atunci dacă notăm

$$x = \sum_{i=1}^k a_i M_i N_i$$

și reducem modulo m_i avem:

$$x = \sum_{j=1}^k a_j M_j N_j \pmod{m_i} \text{ pentru orice } i.$$

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

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

Unicitatea soluției. Fie x' și x'' două soluții atunci

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

deci

$$x = 0 \pmod{M}.$$

12.2 Exerciții rezolvate

Exercițiul 12.2.1 *Să se rezolve sistemul de ecuații:*

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

Rezolvare:

Soluția sistemului de congruențe este dată de formula:

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

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 și m_3 sunt prime între ele.

Calculăm $M = 13 * 47 * 51 = 31161$ și $M_1 = 47 * 51 = 2397, M_2 = 13 * 51 = 663$ și $M_3 = 13 * 47 = 611$.

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

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

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

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

În acest moment, avem toate datele necesare pentru a calcula soluția x a sistemului de congruențe:

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

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

Capitolul 13

Sistemul de cifrare Merkle-Hellman

13.1 Breviar teoretic

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

Definiția 13.1 Un șir de ponderi $\{M_1, \dots, M_n\}$ se numește *supercrescător* dacă:

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

Problema rucsacului supercrescător este ușor de rezolvat folosind următoarea schemă: pentru $k = n, \dots, 1$:

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

Algoritmii de tip rucsac care nu sunt supercrescători nu sunt ușor de rezolvat și nu există nici un algoritm rapid care să rezolve problema. Singura modalitate cunoscută de a determina dacă $b_i = 1$ constă în testarea tuturor soluțiilor. Cei mai rapizi algoritmi de testare au o complexitate exponențială.

Algoritmul Merkle-Hellman se bazează pe această proprietate: *cheia privată* este șirul ponderilor pentru un rucsac supercrescător iar *cheia publică* este șirul ponderilor pentru un rucsac care are aceeași soluție, dar nu este supercrescător. *Merkle* și *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 dispoziție o problemă de tip rucsac supercrescător (cheia privată) cu ponderile $\{M_1, \dots, M_n\}$ atunci aceasta se transformă într-o problemă de tip rucsac normală (cheia publică) cu șirul ponderilor

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

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

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

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

Pentru descifrare destinatarul mesajului cunoaște cheia privată: ponderile originale și valorile lui m și 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 Exerciții rezolvate

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

Rezolvare:

Având la dispoziție cheia privată $\{M_1, \dots, M_n\}$, cheia publică se obține astfel $\{mM_1 \bmod p, \dots, mM_n \bmod p\}$.

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, \dots, 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 $c = 333$.

Exercițiul 13.2.2 Să se descifreze mesajul $C = 4608$ cifrat cu ajutorul algoritmului Merkle-Hellman cu următorii parametri: $n = 9$, cheia privată $\{1, 2, 5, 10, 19, 40, 98, 179, 355\}$, modulul $p = 1717$ și 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 conține 1 pe pozițiile corespunzătoare acestor ponderi, deci se obține 100110001.

Capitolul 14

Sistemul de cifrare RSA

14.1 Breviar teoretic

Algoritmul *RSA* a fost inventat de către *Ron Rivest*, *Adi Shamir* și *Leonard Adleman* și a fost studiat în cadrul unor studii criptanalitice extinse. Securitatea RSA-ului se bazează pe dificultatea factorizării numerelor mari. Cheia publică și cheia privată sunt funcție 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 și privată) se aleg aleatoriu două numere prime mari p și q . Din raționamente de securitate p și q au același ordin de mărime. Se va calcula produsul $n = p \cdot q$. Se va alege apoi, aleatoriu, exponentul public (de cifrare) e astfel ca e și $(p - 1)(q - 1)$ să fie relativ prime. Utilizând algoritmul extins al lui Euclid vom calcula exponentul privat (de descifrare) d astfel ca

$$ed \equiv 1 \pmod{(p - 1)(q - 1)}.$$

Cu alte cuvinte

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

Remarcăm faptul că d și n sunt relativ prime. Perechea (e, n) constituie cheia publică iar (d, p, q) este cheia privată. Cele două numere p și q nu mai sunt necesare la cifrare/descifrare, dar nu vor fi niciodată făcute publice (cunoașterea lor și 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 și 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 operația de padding cu zero. Mesajul cifrat C se va obține prin concatenarea mesajelor C_i care au aproximativ aceeași lungime. Formula de cifrare va fi:

$$C_i \equiv M_i^e \pmod{n}.$$

Pentru a descifra un mesaj se calculează:

$$M_i \equiv C_i^d \pmod{n},$$

deoarece

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

Observația 14.1 Pentru a evita metodele de factorizare cunoscute numerele p și q trebuie să fie numere prime tari. Un număr prim p se numește 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 .

14.2 Exerciții rezolvate

Exercițiul 14.2.1 Se dă numărul $n = 36187829$ despre care se cunoaște faptul că este un produs de două numere cu valoarea $\phi(n) = 36175776$. Factorizați numărul n .

Rezolvare: Folosim relațiile $p + q = n - (p - 1)(q - 1) + 1$ și $p - q = \sqrt{(p + q)^2 - 4n}$. Obținem $p = 5657$ și $q = 6397$.

Exercițiul 14.2.2 Să se cifreze mesajul $M = 3$, utilizând sistemul RSA cu următorii parametri: $N = 187$ (modulul de cifrare), $e = 7$ (coeficientul de cifrare).

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

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

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

Exponentul de descifrare va fi:

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

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

Capitolul 15

Sistemul de cifrare ElGamal

15.1 Breviar teoretic

Algoritmul de cifrare ElGamal este definit de un număr prim p și 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 Exerciții rezolvate

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

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 $16 = p - 1$. Obținem mesajul cifrat $C = (14^7 \bmod 17, 4 \cdot 9^7 \bmod 17) = \{6, 8\}$.

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

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

Capitolul 16

Aritmetica pe curbe eliptice

16.1 Breviar teoretic

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

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

unde a și b sunt constante astfel încât $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ și p este un număr prim, împreună cu un element singular, notat \mathcal{O} și numit punctul de la infinit. Acest punct poate fi privit ca fiind punctul din vârful și de la baza oricărei linii verticale.

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

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

- dacă $x_2 = x_1$ și $y_2 = -y_1$ 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

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

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

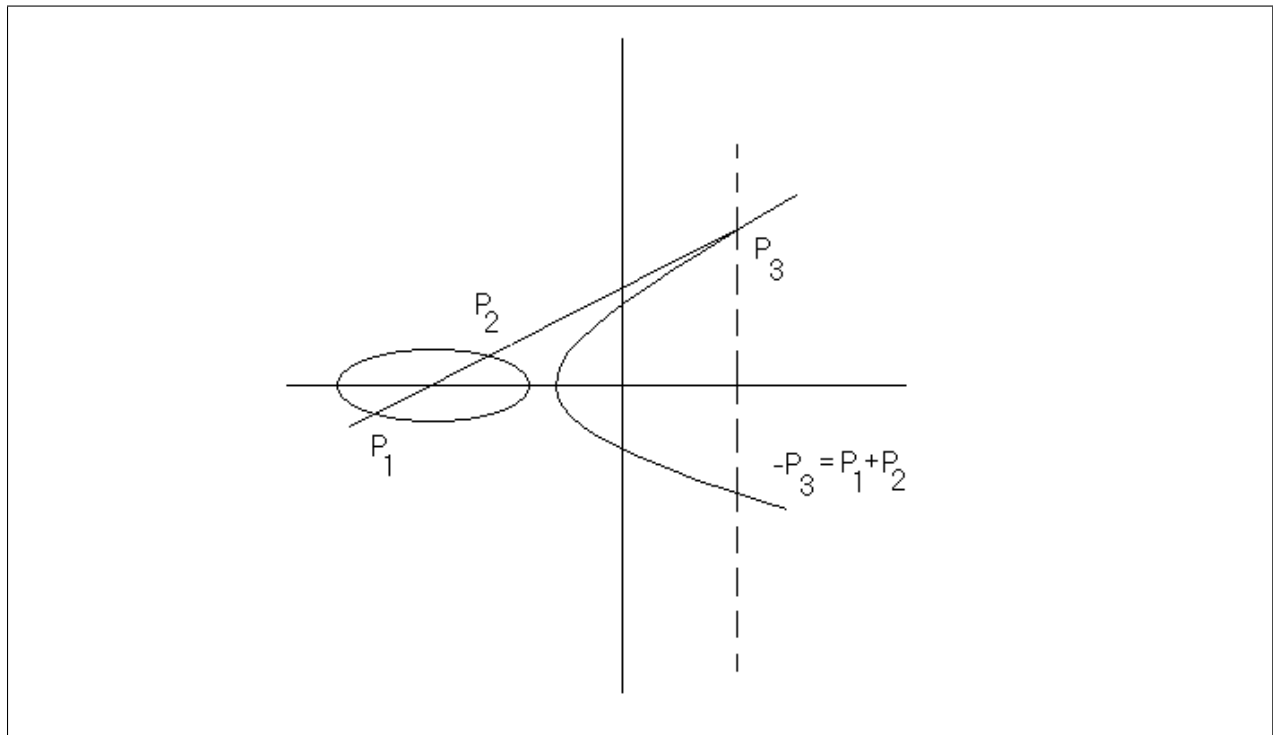


Figura 16.1: Operația de adunare pe o curbă eliptică.

16.2 Exerciții rezolvate

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

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 folosește algoritmul lui Euclid care găsește $33 = 28^{-1} \bmod 71$, 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 reprezintă suma celor două puncte de pe curba eliptică dată sunt $(53, 9)$.

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

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

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 și 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 construiește $\beta = \alpha^x$, cheia publică fiind $\{G, \alpha, \beta\}$.

Pentru a cifra un mesaj M se alege aleatoriu $k \in Z_{|H|}$ și 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 Exerciții rezolvate

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

Rezolvare: Pentru a calcula punctele curbei eliptice se calculează valorile $z = x^3 + x + 6 \pmod{11}$, se vede care din aceste valori sunt reziduri pătratice cu ajutorul teoremei lui Euler (z este reziduu pătratic dacă și numai dacă $z^{\frac{p-1}{2}} \equiv 1 \pmod{p}$) și apoi se calculează rădăcinile pătrate ale acestor reziduri prin formula $y = \pm z^{\frac{p+1}{2}} \pmod{p}$. 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) și se ia ca generator pentru acesta elementul (public) $\alpha = (2, 7)$. Cheia privată de descifrare, notată prin d , este o valoare între 1 și numărul de puncte de pe o curbă eliptică -1 . Cheia publică, notată prin β , se obține din α și exponentul secret d prin formula $\beta = d\alpha$.

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

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

Operația de descifrare pentru a obține 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 obține: $E(M, k) = (4(2, 7), (10, 9) + 4(8, 3)) = ((10, 2), (10, 9) + (2, 4)) = ((10, 2), (3, 5))$

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

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

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 și 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 conține un subgrup ciclic G în care problema logaritmului discret este dificilă. Pe baza cheii private $d \in Z$, se construiește $\beta = d\alpha$, 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 și se construiește 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) și 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 Exerciții rezolvate

Exercițiul 18.2.1 *Se consideră algoritmul Menezes-Vanstone precizat de parametrii $E : y^2 = x^3 + x + 6$ peste Z_{13} . Arătați 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 și 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 după următoarea formulă $e_k(x, k) = (y_0, y_1, y_2)$ unde $y_0 = k \cdot \alpha, (c_1, c_2) = k \cdot \beta, y_i = c_i \cdot x_i \pmod{p}$ 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 și $y_1 = 4 \cdot 3 \bmod 13 = 12$ și $y_2 = 10 \cdot 7 \bmod 13 = 5$. Rezultatul cifrării mesajului $(3, 7)$ cu valoarea aleatoare $k = 4$ este $((9, 4), (12, 5))$.

Bibliografie

- [1] **A. Atanasiu**, *Securitatea Informației, vol. 1, Criptografie*, ed. InfoData, Cluj, 2008.
- [2] **A. Atanasiu**, *Securitatea Informației, 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 și Gh. Oprișan**, *Elemente de Cercetări Operaționale și Criptologie*, Politehnica Press, ISBN 973-8449-006, 2002.
- [6] **E. Simion, V. Preda și A. Popescu**, *Criptanaliza. Rezultate și Tehnici Matematice*, Ed. Univ. Buc., ISBN 973575975-6, 2004.
- [7] **E. Simion**, *Enciclopedie Matematică*, Ediție coordonată de M. Iosifescu și O. Stanasilă, Editura AGIR, ISBN 978-973-720-288-8, pp. 905-944, 2010.
- [8] **B. Schneier**, *Applied Cryptography*, Adison-Wesley, 1998.