CRIPTOGRAFIE

Aplicații

2022

Sistemul de cifrare Cezar

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: $(x - k) \bmod 26$.

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.

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.

Sistemul de cifrare Cezar - Tema

Sa se cifreze mesajul:

“EXISTA O NISA DE SECURITATE IN COMUNICAREA WIRELESS”

utilizand algoritmul Cezar cu cheia k=11

Metoda substitutiei

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

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.

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.

Metoda substitutiei - Tema

Sa se construiasca alfabetul de cifrare cu parola:

“SISCRIPTARE”

Iar apoi sa se cifreze mesajul:

“EXISTA O NISA DE SECURITATE IN COMUNICAREA WIRELESS”

Sisteme de cifrare polialfabetice

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 mod 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 compexitate 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.

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

Pas 3. Conform celor N alfabete reconstruieşte textul clar.

Să se cifreze mesajul WINDS OF CHANGE cu ajutorul algorimtului Vigenère, parola fiind FUTURE.

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

$\mathbf{j}$	$\mathbf{m_j}$	$\mathbf{k_{j(\mathrm{mod}\,6)}}$	$\mathbf{c_j = (m_j + k_{j(\mathrm{mod}\,6)})(\mathrm{mod}\,26)}$
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 cifratt: BCGXJ SKWAU EKJ.

Sisteme de cifrare polialfabetice - Tema

Sa se cifreze mesajul:

“EXISTA O NISA DE SECURITATE IN COMUNICAREA WIRELESS”

cu ajutorul algoritmului Vigenere,
folosind parola CRIPTARE

Metoda transpozitiei

Metoda transpoziţiei asigură, în cadrul sistemelor criptografice, realizarea difuziei: împrăştierea proprietăţilor statistice ale textului clar în textul cifrat. Spre exemplu, în cazul transpoziţiei coloanelor, textul clar se scrie, linie cu linie, într-o formă tabelară cu n coloane, acesta fiind recitit 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).

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.

Metoda transpozitiei - Tema

Sa se cifreze urmatorul mesaj prin metoda transpozitie (N=11):

“EXISTA O NISA DE SECURITATE IN COMUNICAREA WIRELESS”

folosind parola SISCRIPTARE

Sisteme mixte

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.

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

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 .

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 .

Sisteme mixte - Tema

Sa se cifreze urmatorul mesaj:

“EXISTA O NISA DE SECURITATE IN COMUNICAREA WIRELESS”

folosind algoritmul Cezar (k=7) si al transpozitiei $\sigma = (2,1,3)$.

Calcule in corpuri Galois

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.

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 $\{31\}$.

Algoritmul RIJNDAEL - Standardul AES

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.

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 $GF(2^8)$.

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:

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

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

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

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

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

Sistemul de cifrare RSA

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

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

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*.*

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 $q = 6397$.

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

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

Să se descifreze mesajul $C = 130$, *utilizând sistemul RSA cu următorii parametrii:* $N = 187 = 11 \cdot 17$ *(modulul de cifrare),* $e = 7$ *(coeficientul 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: $C^d = 130^{23} = 3 = M \bmod 187$.

Sistemul de cifrare ElGamal

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 $y_2(y_1^x)^{-1} \bmod p$.

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 $y_2 y_1^{-x} \bmod p = 4$.

Sistemul de cifrare Menezes-Vanstone

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:

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

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).