UNIVERSITATEA DIN BUCUREȘTI
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
SPECIALIZAREA CALCULATOARE ȘI TEHNOLOGIA INFORMAȚIEI – SERIA 36

EXAMEN LA DISCIPLINA "CRIPTOGRAFIE ȘI SECURITATE"

- Sesiunea mai/iunie 2023 –

1. Folosind cifrul Playfair, criptați mesajul "COLOCVIU" utilizând cheia secretă "CRIPTOGRAFIE". **(1 p.)**

2. Considerați sistemul de cifrare Hill 2×2 peste Z_{26} în care se folosește cheia de criptare $\begin{pmatrix} D & E \\ E & R \end{pmatrix}$.
a) Care este cheia de decriptare aferentă? **(1 p.)**
b) Decriptați mesajul $C = UUFYDC$. **(1 p.)**

3. Fie generatorul LFSR (Linear Feedback Shift Register) având parametrii $c_4 = 0, c_3 = 0, c_2 = 1, c_1 = 0, c_0 = 1$ și seed-ul $x_4 = 1, x_3 = 0, x_2 = 1, x_1 = 1, x_0 = 0$.
a) Reprezentați grafic LFSR-ul dat. **(1 p.)**
b) Care sunt primii 10 biți generați de LFSR-ul dat? **(1 p.)**
c) Care este periodicitatea maximă a unui LFSR cu 5 stări? **(0.5 p.)**

4. Notăm prin $enc_K(M)/dec_K(M)$ criptarea, respectiv decriptarea, unui mesaj M folosind cifrul OTP (One Time Pad) cu o cheie secretă K.
a) Știind că $enc_K(VASILE) = ILINCA$, calculați $enc_K(ILINCA)$. **(1 p.)**
b) Știind că $enc_K(CINCI) = PATRU$, calculați $enc_K(SAPTE)$. **(1 p.)**
c) Pentru cheia secretă $K = SECRET$, calculați $enc_K\big(dec_K(K)\big)$. **(0.5 p.)**

5. a) Determinați o pereche de chei pentru un sistem RSA cu $n = 119$. **(1 p.)**
b) Pentru perechea de chei determinată anterior, calculați semnătura mesajului $M = 4$. **(1 p.)**

6. Considerăm schema de criptare ElGamal pentru curbe eliptice, în care:

- p – un număr prim mare
- E – o curbă eliptică peste $\mathbb{Z}_p$
- A – un punct de ordin mare al curbei eliptice E
- n – un număr aleator din $\mathbb{Z}_p^*$
- $B = nA$
- $K_{priv} = \{n\}$
- $K_{pub} = \{p, E, A, B\}$

Fie curba eliptică $E: y^2 \equiv x^3 + x + 5 (\mathrm{mod}\ 19)$ peste $\mathbb{Z}_{19}$, având 15 puncte:

$\mathcal{O}, A_1(0,9), A_2(0,10), A_3(1,8), A_4(1,11), A_5(3,4), A_6(3,15), A_7(4,4), A_8(4,15), A_9(11,6),$
$A_{10}(11,13), A_{11}(12,4), A_{12}(12,15), A_{13}(13,7), A_{14}(13,12)$

Punctul $A_1(0,9)$ este un generator al grupului asociat curbei eliptice, deoarece:

$\mathcal{O} = 15A_1, A_2 = 14A_1, A_3 = 13A_1, A_4 = 2A_1, A_5 = 3A_1, A_6 = 12A_1, A_7 = 4A_1, A_8 = 11A_1,$
$A_9 = 6A_1, A_{10} = 9A_1, A_{11} = 8A_1, A_{12} = 7A_1, A_{13} = 10A_1, A_{14} = 5A_1$

Pentru $A = A_9$ și $n = 5$ criptați mesajul $M = A_2$ și decriptați mesajul $C = (A_{13}, A_7)$. **(2 p.)**

SUCCES!

Observații:

- Se vor rezolva, la alegere, probleme ale căror punctaje însumate să totalizeze cel mult 9 puncte (din cele 12 maxim posibile) și se va acorda un punct din oficiu. Rezolvările trebuie să conțină și explicații/calcule, ci nu doar răspunsurile pe care le considerați corecte!

- Pozițiile literelor în alfabetul latin:

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

SUCCES!