UNIVERSITATEA DIN BUCUREȘTI
FACULTATEA DE MATEMATICĂ ȘI INFORMATICĂ
SPECIALIZAREA INFORMATICĂ - SERIA 33

EXAMEN LA DISCIPLINA "SECURITATEA SISTEMELOR INFORMATICE"

- Sesiunea februarie 2024 –

1. Folosind cifrul bifid, criptați-vă numele de familie utilizând $NOTAMAXIMA$ pe post de cheie secretă. (1 p.)

1P

2. Considerăm fiecare dintre cele 26 de litere mari ale alfabetului englez ca fiind codificată prin reprezentarea binară pe 5 biți a poziției sale în alfabet ($A = 00000$, $B = 00001$,..., $M = 01100$,..., $S = 10010$, ..., $V = 10101$, ..., $Z = 11001$) și 6 caractere codificate astfel: $@ = 11010$, $\# = 11011$, $\$ = 11100$, $\% = 11101$, $\wedge = 11110$ și $\& = 11111$. Notăm cu $enc_K(M)$ / $dec_K(C)$ criptarea/decriptarea unui mesaj clar M/mesaj criptat C folosind cifrul Vernam cu cheia secretă K (reprezentarea binară a unui mesaj se obține concatenând reprezentările binare ale caracterelor sale). Rezolvați următoarele cerințe:

a) știind că $enc_K(EXAMENE) = SUBIECT$, calculați $enc_K(SUBIECT)$; (0.5 p.)
b) știind că $enc_K(\&CINCI) = @SAPTE$, calculați $dec_K(\#ZECE\#)$; (1 p.)
c) pentru cheia secretă $K = NOTAZECE$, calculați $enc_K(enc_K(K))$. (0.5 p.)

3. **a)** Calculați o pereche de chei pentru un sistem RSA cu $n = 391$. (1 p.)
b) Pentru $n = 391$ calculați o semnătură RSA, notată cu S, a mesajului $M = 7$ și apoi criptați mesajul $M \cdot S$. (1 p.)

2P

4. Fie generatorul LFSR (Linear Feedback Shift Register) având parametrii $c_4 = 1, c_3 = 0, c_2 = 1, c_1 = 0, c_0 = 1$ și seed-ul $x_4 = 1, x_3 = 1, x_2 = 0, x_1 = 1, x_0 = 0$.

2,5P

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.)

5. **a)** Considerăm schema de criptare ElGamal pentru curbe eliptice, în care:

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

1,5P

Scrieți funcțiile de criptare/decriptare corespunzătoare și demonstrați corectitudinea funcției de decriptare. (1.5 p.)

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

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

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

1P

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

SUCCES!

Pentru $A = A_{11}$ și $n = 5$ criptați mesajul $M = A_8$ și decriptați mesajul $C = (A_8, A_2)$ folosind schema de criptare ElGamal pentru curbe eliptice. (1 p.)

6. **a)** Explicați, pe scurt, problema matematică greu rezolvabilă pe care se bazează protocolul Diffie-Hellman pentru schimbul de chei. (1 p.)
b) Știind faptul că *g* = 2 este o rădăcină primitivă modulo *p* = 11, calculați cheia comună care se obține folosind protocolul Diffie-Hellman cu parametrii publici *p* și *g* pentru valorile secrete *a* = 22 și *b* = 33. (1 p.)

Notă:

- 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!