Criptografie - Tema 8

Popescu Paul - Constantin
Facultatea de Matematică

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

1. Pentru fiecare din șirurile următoare, decideți dacă este supercrescător și determinați toate soluțiile problemei rucsacului cu "volumul" corespunzător:

a) $v = (2, 3, 7, 20, 35, 69), V = 45$
Şirul este supercrescător
Soluţii pentru problema rucsacului: $S_1 = (0, 1, 1, 0, 1, 0)$

b) $v = (1, 2, 5, 9, 20, 49), V = 73$
Şirul este supercrescător
Nu exista soluţii pentru problema rucsacului

c) $v = (1, 3, 7, 12, 22, 45), V = 67$
Şirul **nu** este supercrescător
Soluţii pentru problema rucsacului: $S_1 = (0, 1, 1, 1, 0, 1), S_2 = (0, 0, 0, 0, 1, 1)$

d) $v = ((2, 3, 6, 11, 21, 40), V = 39$
Şirul **nu** este supercrescător
Nu exista soluţii pentru problema rucsacului

e) $v = (4, 5, 10, 30, 50, 101), V = 186$
Şirul este supercrescător
Soluţii pentru problema rucsacului: $S_1 = (0, 1, 0, 1, 1, 1)$

f) $v = (3, 5, 8, 15, 28, 60), V = 43$
Şirul **nu** este supercrescător
Soluţii pentru problema rucsacului: $S_1 = (0, 0, 0, 1, 1, 0)$

2. Pentru un număr natural k determinați un șir supercrescător $(a_0, a_1, \ldots, a_{k-1})$ astfel încât numerele naturale $(a_0, a_1, \ldots, a_{k-1})$ sunt minime. Rezolvați problema rucsacului pentru acest șir și $V = 473$.

Se poate observa că pentru crearea unui şir supercrescător minim putem avea puteri ale lui 2, astfel formând un şir binar:

$$(a_0, a_1, a_2, \ldots) = (1, 2, 4, \ldots) \text{ unde } a_i = 2^i, i \in (0, k-1)$$

În continuare, vom transforma numarul 473 din baza 10 în baza 2:

$$473 = 256 + 128 + 64 + 16 + 8 + 1 = 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^0$$

Rezultă ca sirul supercrescător dorit este: $v = (1, 0, 0, 1, 1, 0, 1, 1, 1)$

3. Alice utilizează un criptosistem Merkle-Hellman pe un alfabet cu 26 de caractere (literele A - Z), unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul $\{34, 51, 58, 11, 39\}$ iar cheia secretă este $(b = 18, m = 61)$. Criptați mesajul **WHY** și apoi decriptați-l.

W $= 22 \rightarrow 10110$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 34 \cdot 1 + 51 \cdot 0 + 58 \cdot 1 + 11 \cdot 1 + 39 \cdot 0 = 103$
H $= 7 \rightarrow 00111$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 34 \cdot 0 + 51 \cdot 0 + 58 \cdot 1 + 11 \cdot 1 + 39 \cdot 1 = 108$
Y $= 24 \rightarrow 11000$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 34 \cdot 1 + 51 \cdot 1 + 58 \cdot 0 + 11 \cdot 0 + 39 \cdot 0 = 85$

Mesajul criptat este 103 108 85.

Calculam $v = (34 \cdot 18, 51 \cdot 18, 58 \cdot 18, 11 \cdot 18, 39 \cdot 18)(\text{mod}61) = (2, 3, 7, 15, 31)(\text{mod}61)$

$103 \cdot 18 \equiv 24(\text{mod}61) \rightarrow (1, 0, 1, 1, 0) = 22 = W$
$108 \cdot 18 \equiv 53(\text{mod}61) \rightarrow (0, 0, 1, 1, 1) = 7 = H$
$85 \cdot 18 \equiv 5(\text{mod}61) \rightarrow (1, 1, 0, 0, 0) = 24 = Y$

Mesajul decriptat este **WHY**.

4. Alice utilizează criptosistemul Rabin cu modulul n = 713 și primește mesajul criptat c = 289. Determinați cele 4 posibilități pentru mesajul în clar corespunzător. Aceeași problemă pentru mesajul criptat c = 200.

$$\lfloor \sqrt{713} \rfloor = 26 \Rightarrow t = \lfloor \sqrt{713} \rfloor + 1 = 27$$
$$t^2 - n = 729 - 713 = 16 = 4^2 = s^2$$
$$p = t - s = 23, q = t + s = 31$$

5. Alice utilizează un criptosistem Merkle-Hellman pe un alfabet cu 26 de caractere (literele A - Z), unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul $\{8, 24, 3, 14, 57\}$ iar cheia secretă este $(b = 23, m = 61)$. Bob dorește să-i trimită lui Alice mesajul **HELLO**. Criptați mesajul.

H $= 7 \rightarrow 00111$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 8 \cdot 0 + 24 \cdot 0 + 3 \cdot 1 + 14 \cdot 1 + 57 \cdot 1 = 74$
E $= 4 \rightarrow 00100$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 8 \cdot 0 + 24 \cdot 0 + 3 \cdot 1 + 14 \cdot 0 + 57 \cdot 0 = 3$
L $= 11 \rightarrow 01011$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 8 \cdot 0 + 24 \cdot 1 + 3 \cdot 0 + 14 \cdot 1 + 57 \cdot 1 = 95$
L $= 11 \rightarrow 010111$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 8 \cdot 0 + 24 \cdot 1 + 3 \cdot 0 + 14 \cdot 1 + 57 \cdot 1 = 95$
O $= 14 \rightarrow 01110$. Se obţine $\sum_{i=0}^{5} \varepsilon_i w_i^A = 8 \cdot 0 + 24 \cdot 1 + 3 \cdot 1 + 14 \cdot 1 + 57 \cdot 0 = 41$

Mesajul criptat este 74 3 95 95 41.