Tema 8

8. a) $(2, 3, 7, 20, 35, 69) = v$, $V = 45$

$2 + 3 = 5 < 7$ $12 + 20 = 32 < 35$

$5 + 7 = 12 < 20$ $32 + 35 = 67 < 69$

=> şirul este supercrescator

$K=5 : v_5 = 69 > 45 \Rightarrow \xi_5 = 0$

$K=4 : v_4 = 35 < 45 \Rightarrow \xi_4 = 1, V = 10$

$K=3 : v_3 = 20 > 10 \Rightarrow \xi_3 = 0$

$K=2 : v_2 = 7 < 10 \Rightarrow \xi_2 = 1, V = 3$

$K=1 : v_1 = 3 = V \Rightarrow \xi_1 = 1, V = 0$ și $\varepsilon_0 = 0$

$\Rightarrow S : (0, 1, 1, 0, 1, 0)$

b) $v = (1, 2, 5, 9, 20, 49), V = 73$

$1+2=3<5 \quad 8+9=17<20$

$3+5=8<9 \quad 17+20=37<49$

$\Rightarrow$ șir supercrescător

$K=5 : v_5 = 49 < 73 \Rightarrow \varepsilon_1 = 1, V = 24$

$K=4 : v_4 = 20 < 24 \Rightarrow \varepsilon_2 = 1, V = 4$

și nu avem cum să mai umplem restul ghiozdanului $\Rightarrow$ problema rucsacului nu are soluție

c) $v = (1, 3, 7, 12, 22, 45), V = 67$

$1+3=4<7 \quad 11+12=23>22$

$4+7=11<12$

⇒ nu este șir supercrescător

avem două soluții:

$67 = 22 + 45 \Rightarrow S_1 = (0, 0, 0, 0, 1, 1)$

$67 = 3 + 7 + 12 + 45 \Rightarrow S_2 = (0, 1, 1, 1, 0, 1)$

d) $v = (2, 3, 6, 11, 21, 40)$, $V = 39$

$2 + 3 = 5 < 6$ $\quad$ $11 + 11 = 22 > 21$

$5 + 6 = 11 \leq 11$

⇒ șirul nu este supercrescător

$k = 5: \ v_5 = 40 > 39$

$k = 4: \ v_4 = 21 < 39 \Rightarrow \varepsilon_4 = 1, \ V = 18$

$k = 3: \ v_3 = 11 < 18 \Rightarrow \varepsilon_3 = 1, \ V = 7$

nu avem cum să obținem o soluție

⇒ Nu există soluție pentru problema rucsacului

e) $v = (4, 5, 10, 30, 50, 101)$. $V = 186$

$4 + 5 = 9 < 10$ $\quad$ $19 + 30 = 49 < 50$

$9 + 10 = 19 < 30$ $\quad$ $49 + 50 = 99 < 101$

⇒ șirul este supercrescător

$K=5 : \vartheta_5 = 101 < 186 \Rightarrow \varepsilon_5 = 1, V = 85$

$K=4 : \vartheta_4 = 50 < 85 \Rightarrow \varepsilon_4 = 1, V = 35$

$K=3 : \vartheta_3 = 30 < 35 \Rightarrow \varepsilon_3 = 1, V = 5$

$K=1 : \vartheta_1 = 5 = V \Rightarrow \varepsilon_1 = 1, \varepsilon_2 = 0, \varepsilon_0 = 0, V = 0$

$\Rightarrow S : (0, 1, 0, 1, 1, 1)$

f) $\vartheta = (3, 5, 8, 15, 28, 60), V = 43$

$3 + 5 = 8 \leq 8$

$8 + 8 = 16 > 15 \Rightarrow$ șirul nu este supercrescator

$K=5 : \vartheta_5 = 60 > 43 \Rightarrow \varepsilon_5 = 0$

$K=4 : \vartheta_4 = 28 < 43 \Rightarrow \varepsilon_4 = 1, V = 15$

$K=3 : \vartheta_3 = 15 = V \Rightarrow \varepsilon_3 = 1, V = 0, \varepsilon_2 = \varepsilon_1 = \varepsilon_0 = 0$

$\Rightarrow S : (0, 0, 0, 1, 1, 0)$

g. $V = 473$, cu $(a_0, a_1, \ldots, a_{k-1})$ - minime și șir supercrescator

Un șir supercrescator minim este format din puterile lui 2 : $(1, 2, 4, 8, \ldots)$

Îl vom scrie pe 473 în baza 2 pentru a descoperi șirul supercrescător căutat:

$473 = 1+8+16+64+128+256$

$= 2^0+2^3+2^4+2^6+2^7+2^8$

$\Rightarrow k=9$ și șirul supercrescător:

$v=(1,2,4,8,16,32,64,128,256)$

și soluția problemei rucsacului:

$S=(1,0,0,1,1,0,1,1,1)$

10. Criptosistemul Merkle-Hellman

$K_e=\{34,51,58,11,39\}$

$K_d=\{18,61\}$, $b=18$, $m=61$

Criptați mesajul WHY

$W=22=16+4+2 \Longrightarrow 10110$

$C_1 = 1\cdot 39+0\cdot 11+58\cdot 1+51\cdot 1+34\cdot 0$

$=39+58+51=148$

$H=7=1+2+4 \longrightarrow 00111$

$C_2 = 0\cdot 39+0\cdot 11+1\cdot 58+1\cdot 51+1\cdot 34$

$=58+51+34=143$

$Y = 24 = 16 + 8 \rightarrow 11000$

$C_3 = 1 \cdot 39 + 1 \cdot 11 + 0 \cdot 58 + 0 \cdot 51 + 0 \cdot 34$

$= 39 + 11 = 50$

Mesaj criptat: 148 143 50

Decriptam mesajul 148 143 50

$\vartheta = Ke \cdot b \,(\mathrm{mod}\ m) = \{34 \cdot 18, 51 \cdot 18, 58 \cdot 18, 11 \cdot 18, 39 \cdot 18\} \,(\mathrm{mod}\ 61)$

$= \{2, 3, 7, 15, 31\}$

- $148 \cdot 18 \,(\mathrm{mod}\ 61) = 2664 \,(\mathrm{mod}\ 61) = 41$

$41 = 31 + 3 + 7 \rightarrow 10110 = 22 \rightarrow W$

- $143 \cdot 18 \,(\mathrm{mod}\ 61) = 12$

$12 = 2 + 3 + 7 \rightarrow 00111 = 7 \rightarrow H$

- $50 \cdot 18 \,(\mathrm{mod}\ 61) = 46$

$46 = 31 + 15 \rightarrow 11000 = 24 \rightarrow Y$

→ mesaj decriptat: WHY

11. Criptosistemul Rabin

$n = 713$, $c = 289$ apoi $c = 200$

$\sqrt{7.13}$ | 26
4 | $46 \cdot 6 = 276$
313
276
=37

$[\sqrt{713}] = 26$

$t = 26 + 1 = 27$

$t^2 - n = (n+1)^2 - n = n^2 + 2 \cdot 26 + 1 - n$

$= -37 + 53 = 16 = 4^2$

$\Rightarrow n = 27^2 - 4^2 = (27-4)(27+4) = 23 \cdot 31$

$\Rightarrow p = 23 \quad q = 31$

$23 \equiv 3 \pmod 4 \qquad 31 \equiv 3 \pmod 4$

$\Rightarrow u \cdot p + v \cdot q = 1$

$u \cdot 23 + v \cdot 31 = 1$

$X_{31} = (1, 0) \qquad X_{23} = (0, 1)$

$31 : 23 = 1$ rest $8 \Rightarrow X_8 = X_{31} - X_{23} = (1, -1)$
23
=8

$23 : 8 = 2$ rest $7 \Rightarrow X_7 = X_{23} - 2X_8 = (-2, 3)$
16
=7

$8 : 7 = 1$ rest $1 \rightsquigarrow X_1 = X_8 - X_7 = (3, -4)$

$\underline{7}$

1

$\Rightarrow u = -4$ și $v = 3$

$r = c^{\frac{p+1}{4}} \pmod{p} = 289^6 \pmod{23}$

$= 13^6 \pmod{23} = (13^2)^3 \pmod{23}$

$= 8 \cdot 8^2 \pmod{23} = 8 \cdot 64 \pmod{23}$

$= 8 \cdot 18 \pmod{23} = 6$

$s = c^{\frac{q+1}{4}} \pmod{q} = 289^8 \pmod{31}$

$= (10^2)^4 \pmod{31} = (100^2)^2 \pmod{31}$

$= (7^2)^2 \pmod{31} = 18^2 \pmod{31}$

$= 14$

$x = ups + vqr \pmod{n}$

$= (-4) \cdot 23 \cdot 14 + 3 \cdot 31 \cdot 6 \pmod{713}$

$= -1288 + 558 \pmod{713}$

$= -730 \pmod{713} = 17$

$y = ups - vqr \pmod{n}$

$= -1288 - 588 \pmod{713} = -1876 \pmod{713}$

$=263$

$x - 17, \ y = 263$

$-x \pmod{n} = -17 \pmod{713} = 696$

$-y \pmod{n} = -263 \pmod{713} = 450$

Rădăcini pentru $c = 289 : \{17, 263, 450, 696\}$

$C = 200$

$p = 23, \ q = 31, \ u = -4, \ v = 3$

$r = c^{\frac{p+1}{4}} \pmod{p} = 200^{6} \pmod{23}$

$= (16^2)^3 \pmod{23} = 3^3 \pmod{23} = 27 \pmod{23}$

$= 4$

$s = c^{\frac{q+1}{4}} \pmod{q} = 200^{8} \pmod{31} = (14^2)^4 \pmod{31}$

$= (10^2)^2 \pmod{31} = 7^2 \pmod{31} = 18$

$x = ups + vqr \pmod{n}$

$= (-4) \cdot 23 \cdot 18 + 3 \cdot 31 \cdot 4 \pmod{713}$

$= -1656 + 372 \pmod{713}$

$= -1284 \pmod{713} = 142 \pmod{713}$

$y = ups - vqr \pmod{n} = -2028 \pmod{713} = 111$

$-x \pmod{n} = -142 \pmod{713} = 571$

$-y \pmod{n} = -111 \pmod{713} = 602$

Rădăcini pentru $c = 200$: $\{111, 142, 571, 602\}$

13. Criptosistemul Merkle-Hellman

$K_e = \{8, 24, 3, 14, 57\}$

$K_d = \{23, 61\}$ $b = 23$, $m = 61$

m: HELLO

$H = 7 = 1+2+4 \longrightarrow 00111$

$C_1 = 0 \cdot 57 + 0 \cdot 14 + 1 \cdot 3 + 24 \cdot 1 + 8 \cdot 1$

$= 3 + 24 + 8 = 35$

$E = 4 \longrightarrow 00100$

$C_2 = 0 \cdot 57 + 0 \cdot 14 + 1 \cdot 3 + 24 \cdot 0 + 8 \cdot 0 = 3$

$L = 11 = 8+2+1 = 01011$

$C_3 = C_4 = 0 \cdot 57 + 1 \cdot 14 + 3 \cdot 0 + 24 \cdot 1 + 8 \cdot 1$

$= 14 + 24 + 8 = 46$

$O = 14 = 8+4+2 = 01110$

$C_5 = 0 \cdot 57 + 1 \cdot 14 + 1 \cdot 3 + 1 \cdot 24 + 0 \cdot 8 = 14 + 3 + 24 = 41$

Mesajul criptat : 35 3 46 46 41