Tema 8 - Criptografie

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

$V = 45$

$2 + 3 = 5 < 7$

$5 + 7 = 12 < 20$

$12 + 20 = 32 < 35$

$32 + 35 = 67 < 69$ => şir sup. cresc.

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

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

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

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

$k = 1 : v_1 = 3 = 3 = V \Rightarrow \xi_1 = 1, \ \xi_0 = 0, \ V = 0$

$S = \{0, 1, 1, 0, 1, 0)$

b) $v = (\underbrace{1, 2}_{3}, 5, 9, 20, 49), \ V = 73$

$3 \quad 8 \quad 17 \quad 37$

v şir sup cresc.

$k = 5 : v_5 = 49 < 73 \Rightarrow \xi_5 = 1, \ V = 24$

$k = 4 : v_4 = 20 < 24 \Rightarrow \xi_2 = 1, \ V = 4$

=> nu mai avem cum să mai umplem restul ghiozdanului,

=> pb. rucs. nu are sol.

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

$1 + 3 = 4 < 7$

$4 + 7 = 11 < 12$

$11 + 12 = 23 > 22$ => şir nu e supercresc.

avem 2 sol. $67 = 22 + 45 \rightarrow S_1 = (0, 0, 0, 0, 1, 1)$

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

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

$2 + 3 = 5 < 6$

$5 + 6 = 11 \leq 11$

$11 + 11 = 22 > 21$ => nu e supercresc.

$k = 5 : v_5 = 40 > 39$

$k = 4 : v_4 = 21 < 39 \Rightarrow \xi_4 = 1 , V = 18$

$k = 3 : v_3 = 11 < 18 \Rightarrow \xi_3 = 1 , V = 7$

=> nu avem cum să obt. o sol => nu există sol. pt. pb rucsac.

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

$4 + 5 = 9 < 10$

$9 + 10 = 19 < 30$

$19 + 30 = 49 < 50$

$49 + 50 = 99 < 101$ => şir supercresc.

$k = 5 : v_5 = 101 < 186 \Rightarrow \xi_5 = 1 , V = 85$

$k = 4 : v_4 = 50 < 85 \Rightarrow \xi_4 = 1 , V = 35$

$k = 3 : v_3 = 30 < 35 \Rightarrow \xi_3 = 1 , V = \cancel{15}\ 5$

$k = 1 : v_1 = 5 \leq 5 \Rightarrow \xi_1 = 1 , \xi_2 = 0 , V = 0$

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

f) $\cancel{v} = (3, 5, 8, 15, 28, 60) , V = 43$

$3 + 5 = 8 < 8$ $8 + 8 = 16 > 15$ => nu e şir supercresc.

~~$8 + 15 = 23 < 28$~~

$23 + 28 = 51 < 60$

$k = 5 : v_5 = 60 > 43 \Rightarrow \xi_5 = 0$

$k = 4 : v_4 = 28 < 43 \Rightarrow \xi_4 = 1 , V = 15$

$k = 3 : v_3 = 15 = V \Rightarrow \xi_3 = 1 , V = 0 ,$

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

9. $V = 473$, cu $(a_0, a_1, \dots, a_{k-1})$ - min
- șir supercresc

$(1, 2, 4, 8, \dots)$ șir supercresc. min. format din puterile lui 2

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

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

$\Rightarrow k = 9$ și $v = (1, 2, 4, 8, 16, 32, 64, 128, 256)$ supercresc.

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

10. Merkle - Hellman

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

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

"WHY"

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

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

$= 39 + 58 + 51 = 148$

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

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

$= 58 + 51 + 34 = 143$

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

$C_3 = 1 \cdot 39 + 1 \cdot 11 + 0 \cdot 51 + 0 \cdot 34 = 50$

Mesaj criptat : 14814350

Decriptăm mesaj

$v = k_e \cdot b \pmod{m} = \{34 \cdot 18, 51 \cdot 18, 58 \cdot 18, 11 \cdot 18, 39 \cdot 18\} \pmod{61}$

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

* $148 \cdot 18 \pmod{61} = 2.664 \pmod{61} = 41$

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

* $143 \cdot 18 \pmod{61} = 12$

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

* $50 \cdot 18 \pmod{61} = 46$

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

11. Robin

$n = 713$, $C = 289$

$$\begin{array}{l|l} \sqrt{7.13} & 26 \\ 4 & 46\cdot 6 = 276 \\ \hline 313 & \\ 276 & \\ \hline = 37 & \end{array}$$

$[\sqrt{713}] = 26$

$t = 26 + 1 = 27$

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

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

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

$\Rightarrow n = 23 \cdot 31 \Rightarrow p = 23$

$q = 31$

$23 \equiv 3 \pmod 4$

$31 \equiv 3 \pmod 4$

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

$u23 + v31 = 1$

$(31, 23) = 1$

$31 = 23\cdot 1 + 8$

$23 = 8\cdot 2 + 7$

$8 = 7\cdot 1 + 1$ $\Rightarrow$ ~~$1 = 8 - 7\cdot 1 =$~~ . $1 = (-4)23 + 3\cdot 31$

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

$= 13^6 \pmod{23} = (13^2)^3 \pmod{23} = 8\cdot 18 \pmod{23} = 6$

$s = c^{\frac{q+1}{4}} \pmod q = 289^8 \pmod{31} = 14$

$x = ups + vqr \pmod n$

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

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

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

$y = ups - vqr \pmod n$

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

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

$= -1876 \pmod{713} = 263$

$x = 17, y = 263$

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

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

$\{17, 263, 450, 696\}$

$\underline{C = 200}$

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

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

$s = c^{\frac{q+1}{4}} \pmod{q} = 200^{8} \pmod{31} = 18$

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

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

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

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

$y = ups - vqr \pmod{713}$

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

$= -2028 \pmod{713} = 111$

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

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

$\{111, 142, 571, 602\}$

13. Merkle - Hellman

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

$k_d = \{23, 61\}$

$b = 23, \quad m = 61$

m : HELLO

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

$C_1 = 0\cdot 57 + 0\cdot 14 + 1\cdot 3 + 24\cdot 1 + 8\cdot 1 = 35$

$E = 4 \Rightarrow 00100$

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

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

$C_3 = C_4 = 0\cdot 57 + 1\cdot 14 + 3\cdot 0 + 24\cdot 1 + 8\cdot 1 = 46$

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

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

C: 35 3 46 46 41