Tema 1:

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

3 > 2

7 > 2+3=5

20 > 5+7=12

35 > 12+20=32

69 > 32+35=67

=> șir este supercreșător

Pentru V = 45

45 < 69 => $\varepsilon_5 = 0$

45 > 35 => $\varepsilon_4 = 1$

V = 45 - 35 = 10

10 < 20 => $\varepsilon_3 = 0$

10 > 7 => $\varepsilon_2 = 1$

V = 10 - 7 = 3

3 ≥ 3 => $\varepsilon_1 = 1$

0 ∈ 2 => $\varepsilon_0 = 0$

ε = (0, 1, 1, 0, 1, 0)

Soluție unică (35, 7, 3)

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

3

8

17

37 < 49

=> este supercrescătoare

Pentru $V = 73$

$73 > 49 \Rightarrow \varepsilon_5 = 1$

$V = 73 - 49 = 24$

$24 > 20 \Rightarrow \varepsilon_4 = 1$

$V = 24 - 20 = 4$

$4 < 9 \Rightarrow \varepsilon_3 = 0$

$4 < 5 \Rightarrow \varepsilon_2 = 0$

$4 > 2 \Rightarrow \varepsilon_1 = 1$

$V = 4 - 2 = 2$

$2 > 1 \Rightarrow \varepsilon_0 = 1$

nu putem lua

fără $49 \Rightarrow \varepsilon_5 = 0$

$73 > 20 \Rightarrow \varepsilon_4 = 1$

$V = 73 - 20 = 53$

$53 > 9 \Rightarrow \varepsilon_3 = 1$

$V = 53 - 9 = 44 =$

$44 > 5 \Rightarrow \varepsilon_2 = 1$

$V = 44 - 5 = 39$

$39 > 2 \Rightarrow \varepsilon_1 = 1$

$V = 39 - 2 = 37$

$37 > 1 \Rightarrow \varepsilon_0 = 1$

$V = 37 - 1 = 36$

nu putem lua

Nu există soluție pentru $V = 73$ cu elemente distincte

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

4

11

23 > 22 $\Rightarrow$ nu este supercrescător

Pentru $V = 67$

$67 > 45 \Rightarrow \varepsilon_5 = 1$

$V = 67 - 45 = 22$

$22 \geq 22 \Rightarrow \varepsilon_4 = 1$

$V = 22 - 22$

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

Acum $\varepsilon_5 = 0$

$67 > 22 \Rightarrow \varepsilon_4 = 1$

$V = 67 - 22 = 45$

$45 > 12 \Rightarrow \varepsilon_3 = 1$

$V = 45 - 12 = 33$

$33 > 7 \Rightarrow \varepsilon_2 = 1$

$V = 33 - 7 = 26$

$26 > 3 \Rightarrow \varepsilon_1 = 1$

$V = 26 - 3 = 23$

$23 > 1 \Rightarrow \varepsilon_0 = 1$

$V = 23 - 1 = 22$

nu putem lua

$\varepsilon_5 = 1$ dar $\varepsilon_4 = 0$

$22 \geq 12 \Rightarrow \varepsilon_3 = 1$

$V = 22 - 12 = 10$

$10 > 7 \Rightarrow \varepsilon_2 = 1$

$V = 10 - 7 = 3$

$3 \geq 3 \Rightarrow \varepsilon_1 = 1$

$V = 3 - 3 = 0 \Rightarrow \varepsilon_0 = 0$

$\varepsilon = (0, 1, 1, 1, 0, 1)$

Soluții $\{45, 22\}$ și $\{45, 12, 7, 3\}$

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

5

$11 \leq 11 \Rightarrow$ nu este supercreștător

Dă $V = 39$

$39 < 40 \Rightarrow \varepsilon_5 = 0$

$39 > 21 \Rightarrow \varepsilon_4 = 1$

$V = 39 - 21 = 18$

$18 > 11 \Rightarrow \varepsilon_3 = 1$

$V = 18 - 11 = 7$

$7 > 6 \Rightarrow \varepsilon_2 = 1$

$V = 7 - 6 = 1$

$1 < 2, 3 \Rightarrow$ nu putem lua

$21 + 11 + 6 + 1$ nu e valid

$21 + 11 + 6 = 38 \neq 39$

$21 + 6 + 3 + 2 \neq 39$

Concluzie: Nu există soluție pentru $V = 39$

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

~~$186 = 101 + 50 + 10 + 5 + 4$~~

~~$\varnothing$~~

$5 > 4$

$10 > 9$

$30 > 19$

$50 > 49$

$101 > 99$

$\Rightarrow$ este supercrescător

$186 \geq 101 \Rightarrow \varepsilon_5 = 1$

$V = 186 - 101 = 85$

$85 \geq 50 \Rightarrow \varepsilon_4 = 1$

$V = 85 - 50 = 35$

$35 \geq 30 \Rightarrow \varepsilon_3 = 1$

$V = 35 - 30 = 5$

$10 > 5 \Rightarrow \varepsilon_2 = 0$

$5 \leq 5 \Rightarrow \varepsilon \Rightarrow \varepsilon_1 = 1$

$V = 5 - 5 = 0 \Rightarrow \varepsilon_0 = 0$

$\varepsilon = (0, 1, 0, 1, 1, 1)$

$50 + 30 + 10 + 5 + 4 = 99 < 186$

$\Rightarrow$ soluție unică $\{101, 50, 30, 5\}$

*) $(3, 5, 8, 15, 28, 60)$ $V = 43$

$8 = 8 \Rightarrow$ nu este supercrescător

$43 < 60 \Rightarrow \varepsilon_5 = 0$

$43 > 28 \Rightarrow \varepsilon_4 = 1$

$V = 43 - 28 = 15$

$15 \geq 15 \Rightarrow \varepsilon_3 = 1$

$V = 15 - 15 = 0$

$\varepsilon = (0, 0, 0, 1, 1, 0)$

$28 + 8 + 5 + 2 = 43$ (nu există 2)

$28 + 8 + 5 + 3 = 44$

Soluție unică $\{28, 15\}$

9) k $(a_0, a_1, \ldots a_{k-1})$

$a_0, a_1, \ldots, a_{k-1}$ șirul minimal. Rez prob rucsacului pt

acest și $V = 473$

$a_0 = 1$

$a_1 > a_0 \Rightarrow a_1 = 2$

$a_2 > a_0 + a_1 = 3 \Rightarrow a_2 = 4$

$a_3 > a_2 + a_1 + a_0 = 7 \Rightarrow a_3 = 8$

16

32

64

128

$a_8 > a_0 + \ldots + a_7 = 255 \Rightarrow$ ~~256~~ $a_8 = 256$

Șirul supercrescător minimal este

$\{1, 2, 4, 8, 16, 32, 64, 128, 256\}$

$k = 9$, suma $= 511 \rightarrow a_9 = 511$

b) $V = 473$

$473 > 256 \Rightarrow \varepsilon_8 = 1$

$V = 473 - 256 = 217$

$217 \geq 128 \Rightarrow \varepsilon_7 = 1$

$V = 217 - 128 = 89$

$89 > 64 \Rightarrow \varepsilon_6 = 1$

$V = 89 - 64 = 25$

$25 < 32 \Rightarrow \varepsilon_5 = 0$

$25 > 16 \Rightarrow \varepsilon_4 = 1$

$V = 25 - 16 = 9$

$9 > 8 \Rightarrow \varepsilon_3 = 1$

$V = 9 - 8 = 1$

$1 < 4,2 \Rightarrow \varepsilon_2 = \varepsilon_1 = 0$

$1 \in 1 \Rightarrow \varepsilon_0 = 1$

$V = 1 - 1 = 0$

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

Șirul supercrescător minimal = {1, 2, 4, 8, 16, 32, 64, 128, 256}

Soluția pentru $V = 473$: {256, 128, 64, 16, 8, 1}

10 Merkle-Hellman pe un alfabet de 26 caractere (A - Z)

unități mesaj un caracter

$k_{ext} = \{34, 51, 58, 11, 39\}$

$k_d = (b = 18; m = 61)$

Criptați WHY și apoi decriptați

W - 22 $\quad 22 = 16 + 4 + 2 = \overline{10110}$

H - 7 $\quad 7 = 4 + 2 + 1 = \overline{00111}$

Y - 24 $\quad 24 = 16 + 8 = \overline{11000}$

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

$= 51 + 58 + 39 = 148$

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

$= 34 + 51 + 58 = 143$

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

$= 11 + 39 = 50$

XHY ⟶ (148) (143) (50)

$K_e = (34, 51, 58, 11, 39)$

$k = 18 \quad m = 61$

$148 \cdot 18 \pmod{61} = 41 \longrightarrow 32 + 8 + 1 \Longrightarrow (1,0,1,0,0,1)$

$V = (34 \cdot 18, 51 \cdot 18, 58 \cdot 18, 11 \cdot 18, 39 \cdot 18) \pmod{61}$

$= (2, 3, 7, 15, 31)$

$V = (31, 15, 7, 3, 2)$

$m_1 = 148 \cdot 18 \pmod{61} \equiv 41 = 31 + 7 + 3 = \overline{10110}$

⟶ 22 = W

$m_2 = 58 \cdot 18 \pmod{61} \equiv 7 \longrightarrow \overline{0,0,1,0,0} \longrightarrow 4$

$143 \cdot 18 \pmod{61} \equiv 12 = 8 + 4 \longrightarrow \overline{0,1,1,0,0} \longrightarrow$

$7 + 3 + 2 \longrightarrow \overline{00111} \longrightarrow$

⟶ 7 = H

$m_3 = 50 \cdot 18 \pmod{61} \equiv 46 = 31 + 15 \longrightarrow \overline{11000} \longrightarrow$

⟶ 24 = Y

11 $n = 713$

$a = 289$ și apoi $a = 200$

$\sqrt{7\,13}$ | 2 6

4 | $4\underline{6} \cdot \underline{6}$

313

276

37

$t = 27$

$t^2 - n = 27^2 - 713 = (26+1)^2 - 713 =$

$= 26^2 + 52 + 1 - 713 = 53 - 37 = 16 = 4^2$

$n = 27^2 - 4^2 = (27-4)(27+4) = 231$

$(27+4)(27-4) = 31 \cdot 23$

$\downarrow$ p $\quad \downarrow$ q

$1 = \underbrace{3 \cdot 31}_{93} - \underbrace{4 \cdot 23}_{92}$

$u = 3 \quad v = (-4)$

$r = 289^{\frac{31+1}{4}} \pmod{31} = 289^8 \pmod{31} \equiv 14$

$s = 289^{\frac{23+1}{4}} \pmod{23} = 289^6 \pmod{23} \equiv 6$

$x = 3 \cdot 31 \cdot 6 \pmod{713} \equiv 558 \pmod{713} \equiv 558$

$y = (-4) \cdot 23 \cdot 14 \pmod{713} \equiv -1288 \pmod{713} \equiv 138$

$-x \pmod{713} = -558 \pmod{713} \equiv 155$

$-y \pmod{713} = -138 \pmod{713} \equiv 575$

cele 4 posibilități pentru mesaje {558, 155, 138, 575}

~~d~~ = 200

$r = 200^8 \pmod{31} \equiv 18$

$s = 200^6 \pmod{23} \equiv 4$

$x = 3 \cdot 31 \cdot 4 \pmod{713} \equiv 372 \pmod{713} \equiv 372$

$y = (-4) \cdot 23 \cdot 18 \pmod{713} \equiv -1656 \pmod{713} \equiv 483$

~~-x = 7~~ $-x \pmod{713} \equiv -372 \pmod{713} \equiv 341$

$-y \pmod{713} \equiv -483 \pmod{713} \equiv 230$

cele 4 posibilități pentru mesaje {372, 341, 483, 230}

12 $n = 713$

$d = 289$

(de la exercițiul anterior) => $p = 31$ $q = 23$

$u = 3$ ~~v = 5~~ $v = -4$

$r = 289^8 \pmod{31} \equiv 14$

$s = 289^6 \pmod{23} \equiv 6$

$x = 558$

$y = 130$

$-x = 155$

$-y = 575$

{558, 155, 138, 575}

13 AA-HH 26 (A-Z)

un caracter mesajele

ale exercițiului anterior?

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

$K_d = (b = 23, n = 61)$

criptați HELLO

H = 7 ⇒ 00111 = 1·8 + 1·24 + 1·3 + 0·14 + 0·57

= 8 + 24 + 3 = 35

E = 4 → 00000 = 0·8 + 0·24 + 1·3 + 0·14 + 0·57

= 3

L = 11 → 01011 = 1·8 + 1·24 + 0·3 + 1·14 + 0·57

= 8 + 24 + 14 = 46

O = 14 → 01110 = 0·8 + 1·24 + 1·3 + 1·14 + 0·57

= 24 + 3 + 14 = 41

HELLO → (35) 3 (46) (46) (41)