Tema 8 - Criptografie

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

$2<3$
$5<7$
$12<20$
$32<35$
$67<69$

$\Rightarrow$ DA, șir supercrescător

problema rucsacului

$45 = 3+7+35$

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

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

$1<2$
$3<5$
$8<9$
$17<20$
$37<49$

$\Rightarrow$ șir supercrescător

problema rucsacului:

$(1,2,5,9,20,49)$
$v_0\ v_1\ v_2\ v_3\ v_4\ v_5$

$k=5$ $\quad 49 \leq 73 \Rightarrow V=24$, $\varepsilon_5=1$

$k=4$ $\quad 20 \leq 24 \Rightarrow V=4$, $\varepsilon_4=1$

$k=3$ $\quad 9>4 \Rightarrow \varepsilon_3=0$

$k=2$ $\quad 5>4 \Rightarrow \varepsilon_2=0$

$k=1$ $\quad 2 \leq 4 \Rightarrow V=2$, $\varepsilon_1=1$

$k=0$ $\quad 1 \leq 2 \Rightarrow V=1$, $\varepsilon_0=1$

$1+2+5+9+20+49 = 86 > 73$
$49+20 = 69 < 73$
$49+20+9 = 78 > 73$
$49+20+5 = 74 > 73$
$49+20+2 = 71 < 73$
$49+20+2+1 = 72 < 73$

$\Rightarrow (1,1,0,0,1,1)$, dar ne rămâne un 1 $\Rightarrow$ nu e soluție pentru $V=73$
(suma dă 74)

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

$1<3$
$4<7$
$11<12$
$23>22$ $\Rightarrow$ nu este șir supercresc.

problema rucsacului:

I. $64 = 22 + 45 \Rightarrow (0,0,0,0,1,1)$

II. $64 = 45 + 12 + 3 + 4 \Rightarrow (0,1,1,1,0,1)$

(d) $(2,3,6,11,21,40)$, $V = 38$

$2 < 3$

$5 < 6$

$11 = 11 \Rightarrow$ nu este șir supercrescător

problema rucsacului:

nu există soluție pentru $V = 39$:

$21 + 11 + 6 = 38 < 39$

$40 > 39$

$2 + 6 + 11 + 21 = 40 > 39$

$21 + 11 = 32 < 39$

$11 + 6 + 3 + 2 = 22 < 39$

$11 + 6 + 3 + 21 + 21 = 43 > 39$

~~$\Rightarrow (0,1,1,1,1,1)$~~

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

$4 < 5$

$9 < 10$

$19 < 30$

$49 < 50$

$99 < 101$

$\Rightarrow$ șir supercrescător

problema rucsacului:

$186 = 101 + 50 + 30 + 5 \Rightarrow (0,1,0,1,1,1)$

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

$3 < 5$

$8 = 8 \Rightarrow$ nu este șir supercrescător

problema rucsacului:

$43 = 28 + 15 \Rightarrow (0,0,0,1,1,0)$

g. k - număr natural

$(a_0, a_1, \dots a_{k-1})$ supercrescător al $a_0, \dots a_{k-1}$ minime

problema rucsacului, $V = 473$

pentru a obține cele mai mici valori termenul actual va fi suma termenilor anteriori $+1$:

$a_0 = 1$

$a_1 = 1 + 1 = 2$

$a_2 = 1 + 2 + 1 = 4$

$a_3 = 1 + 2 + 4 + 1 = 8$

$a_4 = 1 + 2 + 4 + 8 + 1 = 16$

$a_5 = 32$

$a_6 = 64$

$a_7 = 128$

$a_8 = 256$

$\rightarrow k = 9$

$\Rightarrow (1,2,4,8,16,32,64,128,256)$

$1 < 2$

$3 < 4$

$7 < 8$

$15 < 16$

$31 < 32$

$63 < 64$

$127 < 128$

$255 < 256$

$\Rightarrow$ șir supercrescător

problema rucsacului: $473 = 256+128+64+16+8+1 \Rightarrow (1,0,0,1,1,1,0,1,1,1)$

10. criptasistem Merkle-Hellman

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

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

mesaj "WHY" - criptare + decriptare

- criptare mesaj:

$W = 22 \longrightarrow \overline{10110}_{(2)} \Rightarrow W = 0\cdot 34 + 1\cdot 51 + 1\cdot 58 + 0\cdot 11 + 1\cdot 39$

$22:2 = 11$ r0 $\quad W = 0+51+58+0+39$

$11:2 = 5$ r1 $\quad W = 148$

$5:2 = 2$ r1

$2:2 = 1$ r0

$1:2 = 0$ r1

$H = 7 \longrightarrow \overline{00111}_{(2)} \Rightarrow H = 1\cdot 34 + 1\cdot 51 + 1\cdot 58 + 0\cdot 11 + 0\cdot 39$

$7:2 = 3$ r1 $\quad H = 34+51+58$

$3:2 = 1$ r1 $\quad H = 143$

$1:2 = 0$ r1

$Y = 24 \longrightarrow \overline{11000}_{(2)} \Rightarrow Y = 0\cdot 34 + 0\cdot 51 + 0\cdot 58 + 1\cdot 11 + 1\cdot 39$

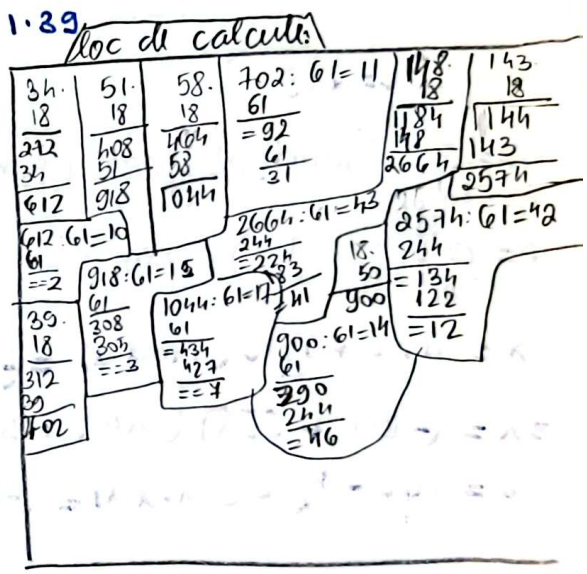
$24:2 = 12$ r0 $\quad Y = 11+39$

$12:2 = 6$ r0 $\quad Y = 50$

$6:2 = 3$ r0

$3:2 = 1$ r1

$1:2 = 0$ r1



mesajul criptat este: 148; 143; 50.

- decriptare mesaj:

148; 143; 50.

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

$\Rightarrow v = \{2, 3, 7, 15, 31\} = \{31, 15, 7, 3, 24\}$

$c_1 = 148 \Rightarrow 148\cdot 18 \pmod{61} = 41 \rightarrow$ înlocuim în $v \Rightarrow (1,0,1,1,0) = 22 \Rightarrow W$

$c_2 = 143 \Rightarrow 143\cdot 18 \pmod{61} = 12 \rightarrow$ înlocuim în $v \Rightarrow (0,0,1,1,1) = 7 \Rightarrow H$

$c_3 = 50 \Rightarrow 50\cdot 18 \pmod{61} = 46 \rightarrow$ înlocuim în $v \Rightarrow (1,1,0,0,0) = 24 \Rightarrow Y$

mesaj: "WHY"

11. criptosistemul Rabin.

$n = 713$

mesaj criptat $c = 289$

a) dat cele 4 posibilități pentru mesajul în clar

b) același pb. pt $c = 200$

a) $\sqrt{713}$

7.13	26
4	$4 \cdot 6 \times 46 = 276$
313	
276	
=37	

$[\sqrt{713}] = 26$

$\Rightarrow t = 27$

$t^2 - n = 27^2 - 713 = 26^2 + 52 + 1 - 713 = -37 + 53 = 16 = 4^2$

$\Rightarrow n = 27^2 - 4^2 = \underbrace{23}_{p} \cdot \underbrace{31}_{q} \Rightarrow kd = (23, 31)$

$p = 23 \equiv 3 \pmod 4$

$q = 31 \equiv 3 \pmod 4$

$1 = 8 \cdot 31 - 4 \cdot 23 \Rightarrow u = -4$

$v = 3$

$c = 289$

$r = c^{\frac{p+1}{4}} \pmod p = 289^6 \pmod{23} = (13^2)^3 = (169)^3 = 8 \cdot 8^2 = 8 \cdot 64 = 8 \cdot 18 = 6$

$b = c^{\frac{q+1}{4}} \pmod q = 289^8 \pmod{31} = (17^2)^4 = (289)^4 = (7^2)^2 = (49)^2 = 18^2 = 14$

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

$\Rightarrow x = (-1288 + 558) \pmod{713} = -730 \pmod{713} = -17 = 696$

$y = upb - vqr \pmod n = (-1288 - 558) \pmod{713} = 1846 \pmod{713} = 420$

$-x = 17$

$-y = -420 = 293$

$\Rightarrow$ cele patru posibilități de decriptare sunt:

$x = 696;\ -x = 17;\ y = 420;\ -y = 293.$

b) $c = 200$

$r = 200^6 \pmod{23} = (16^2)^3 = 256 \cdot 256^2 = 3 \cdot 3^2 = 3 \cdot 9 = 27 = 6$

$b = 200^8 \pmod{31} = (14^2)^4 = (196^2)^2 = (10^2)^2 = 100^2 = 7^2 = 49 = 18$

$\Rightarrow x = (-4 \cdot 23 \cdot 18 + 3 \cdot 31 \cdot 6) \pmod{713} = (-1656 + 558) \pmod{713} = -385 = 328$

$y = (-1656 - 558) \pmod{713} = -75 = 638 \Rightarrow -y = 75$

$-x = 385$

$\Rightarrow$ cele 4 posibilități sunt: $x = 328; -x = 385; y = 638; -y = 75.$

12. Criptosistemul Rabin.

$n = 713$

$C = 289$

ex este identic cu cel făcut anterior.

13. criptosistemul Merkle-Hellman.

$k_c = (8, 24, 3, 14, 57)$

$k_d = (b = 23, m = 61)$

criptare mesaj "HELLO"

$H = 7 \rightarrow \overline{00111}_{(2)} \Rightarrow H = 1 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57$

$H = 8 + 24 + 3$

$H = 35$

$E = 4 \rightarrow \overline{00100}_{(2)} \Rightarrow E = 0 \cdot 8 + 0 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57$

$E = 3$

$L = 11 \rightarrow \overline{01011}_{(2)} \Rightarrow L = 1 \cdot 8 + 1 \cdot 24 + 0 \cdot 3 + 1 \cdot 14 + 0 \cdot 57$

$L = 8 + 24 + 14$

$L = 46$

$L = 11 \Rightarrow 46$

$O = 14 \Rightarrow \overline{01110}_{(2)} \Rightarrow O = 0 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 1 \cdot 14 + 0 \cdot 57$

$O = 24 + 3 + 14$

$O = 41$

$\Rightarrow$ mesajul criptat este: 35; 3; 46; 46 și 41.