12. 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.

$H = 7 = 2^2 + 3 = 2^2 + 2^1 + 1 = 2^2 + 2^1 + 2^0 \to 00111 \Rightarrow$

$\Rightarrow 1 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57 = \boxed{35}$

$E = 4 = 2^2 \to 00100 \Rightarrow$

$\Rightarrow 1 \cdot 3 = \boxed{3}$

$L = 11 = 2^3 + 3 = 2^3 + 2^1 + 2^0 \to 01011$

$L = 11 \to 01011$

$\Rightarrow 8 + 24 + 0 \cdot 3 + 14 = \boxed{46} \times 2$

$O = 14 = 2^3 + 2^2 + 2^1 \to 01110$

$\Rightarrow 0 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 1 \cdot 14 + 0 = \boxed{41}$

$\{35, 3, 46, 46, 41\}$

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

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

① supercresc + det. sol. pb-rucs. cu „vol" coresp.

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

$2+3=5<7$
$7+5=12<20$
$12+20=32<35$
$32+35=67<69$
$\Big\}$ $\Rightarrow$ şirul este supercresc.

$V = 45 = 35+3+7$

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

$1<2 \Rightarrow 1+2=3<5 \Rightarrow 3+5=8<9 \Rightarrow 8+9=17<20 \Rightarrow 17+20=37<49 \Rightarrow$ supercresc.

$V_5 < V \Rightarrow V = V - V_5 = 73-49 = 24$, $\varepsilon_5 = 1$

$V_4 < V \Rightarrow V = 24-4 = 4$, $\varepsilon_4 = 1$

$V_3 > V \Rightarrow \varepsilon_3 = 0$

$V_2 > V \Rightarrow \varepsilon_2 = 0$

$V_1 < V \Rightarrow V = 4-2 = 2$, $\varepsilon_1 = 1$

$V_0 < V \Rightarrow V = 2-1 = 1$, $\varepsilon_0 = 1$

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

$1<3$
$4<7$
$11<12$
$23>22$
$55>45$
$\Big\}$ $\Rightarrow$ nu este supercresc.

$V = 45+12$

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

$2<3$, $5<6$, $11 \leq 11$, $22>21$, $43>40 \Rightarrow$ nu e superc.

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

$4<5$, $9<10$, $19<30$, $49<50$, $99<101 \Rightarrow$

$\Rightarrow$ supercresc.

$v_5 < v \Rightarrow v = 85$, $\varepsilon_5 = 1$

$v_4 < v \Rightarrow v = 35$, $\varepsilon_4 = 1$

$v_3 < v \Rightarrow v = 5$, $\varepsilon_3 = 1$

$v_2 > v \Rightarrow \varepsilon_2 = 0$

$v_1 < 5 \Rightarrow v = 0$, $\varepsilon_1 = 1$, $\varepsilon_0 = 0$

$v = 5 + 30 + 50 + 101$

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

$3<5$, $8 \leq 8$, $16>15$, $31>28$, $59<60 \Rightarrow$ nu e supercresc.