Criptografie-Tema9

guzurazvan

May 2024

24. 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.

Rezolvare:
H = 7 = $00111_{(2)} \Rightarrow c_1 = 1 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57 = 35$
E = 4 = $00100_{(2)} \Rightarrow c_2 = 0 \cdot 8 + 0 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57 = 3$
L = 11 = $01011_{(2)} \Rightarrow c_3 = 8 + 24 + 14 = 46$
L = 11 $\Rightarrow c_4 = 46$
$O = 14 = 01110_{(2)} \Rightarrow c_5 = 24 + 3 + 14 = 41$

$\Rightarrow$ Mesajul criptat = {35, 3, 46, 46, 41}