Temă L9

③ 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 k_e={34, 51, 58, 11, 39}, iar cheia secretă este k_d=(u=18, m=61). Criptați mesajul "WHY" și apoi decriptați-l.

Soluție:

Criptarea:

$W = 22 \to 1\,0\,1\,1\,0 \Rightarrow c_1 = 0\cdot34+1\cdot51+1\cdot58+0\cdot11+1\cdot39 = 148$

$H = 7 \to 0\,0\,1\,1\,1 \Rightarrow c_2 = 1\cdot34+1\cdot51+1\cdot58+0\cdot11+0\cdot39 = 143$

$Y = 24 \to 1\,1\,0\,0\,0 \Rightarrow c_3 = 0\cdot34+0\cdot51+0\cdot58+1\cdot11+1\cdot39 = 50$

Decriptarea:

Calculăm $v=(34\cdot18, 51\cdot18, 58\cdot18, 11\cdot18, 39\cdot18) \pmod{61}$

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

$148\cdot18 = 41 \to (1,0,1,1,0) = 22 = \boxed{W}$

$143\cdot18 = 12 \to (0,0,1,1,1) = 7 = \boxed{H}$

$50\cdot18 = 46 \to (1,1,0,0,0) = 24 = \boxed{Y}$