TEMA 7

25. Alice și Bob doresc să comunice folosind criptosistemul RSA. Alice alege numerele prime $p=7$, $2=11$ pentru a-și determina cheile de criptare/decriptare și alege exponentul de decriptare $d>1$ minimul posibil.

a) Aflați cheia de criptare (n,e) a lui Alice.

b) Bob îi transmite mesajul B!BTBL. Știind că lungimea blocurilor la citire este 1 și la scriere 2, decriptați textul.

a) $p=7$, $2=11$

$n = 7 \cdot 11 = 77$

$\varphi(n) = (p-1)(2-1) = 6 \cdot 10 = 60$

Alegem un nr. $e \in \{3,4,\dots,59\}$ prim cu 60

3, 4, 5, 6 nu sunt prime cu 60, dar 7 este $\Rightarrow e=7$

Calculăm $d \in \{2,3,4,\dots,59\}$ a.î. $d \cdot e \equiv 1 \pmod{60} \Rightarrow$

$\Rightarrow d = 43$

$(n,e) = (77,7)$

b) $B! = 1 \cdot 30 + 28 = 58 \Rightarrow m = 58^{43} \bmod 77 = 16 = Q$

$BT = 1 \cdot 30 + 19 = 49 \Rightarrow m = 49^{43} \bmod 77 = 70 = K$

$BL = 1 \cdot 30 + 11 = 41 \Rightarrow m = 41^{43} \bmod 77 = 6 = G$

Textul în clar este QKG.