Știind că lungimea blocurilor la citire este 1 și la scriere este 2, decriptați textul.

12. Șeful vostru de grupă a decis să comunice cu voi folosind criptosistemul RSA. Ați ales cheia publică Ke = (n = 1189, e = 747).
   c) Determinați-vă cheia privată.
   d) Știind că lungimea j a blocurilor în clar verifică $N^j \leq n \leq N^{j+1}$ și lungimea blocurilor criptate este dată de l = j + 1, decriptați textul **BFCAFNBIW**, unde N este lungimea alfabetului.

$K_e = (n = 1189, e = 747)$

$\sqrt{1189} \mid 34$
9
289
256
133
$64 \cdot 4 = 256$

$[\sqrt{1189}] = 34 \Rightarrow [\sqrt{1189}] + 1 = 35$

$t = 35 \Rightarrow 35^2 - 1189 = 1225 - 1189 = 36 =$
$= 6^2 = s^2 \Rightarrow s = 6 \Rightarrow$

$\Rightarrow n = (t-s)(t+s) = (35-6)(35+6) = \underbrace{29}_{p} \cdot \underbrace{41}_{q}$

$\varphi(n) = (p-1)(q-1) = 28 \cdot 40 = 1120$

$d \cdot e \equiv 1 \pmod{\varphi(n)} \Leftrightarrow d \cdot 747 \equiv 1 \pmod{1120} \Leftrightarrow$

$\Leftrightarrow d \equiv 747^{-1} \pmod{1120}$

$1120 = 1 \cdot 747 + 373 \Rightarrow x_{373} = x_{1120} - 1 \cdot x_{747} = (1,0) - (0,1) = (1,-1)$
$747 = 2 \cdot 373 + 1 \Rightarrow x_1 = x_{747} - 2 \cdot x_{373} = (0,1) - (2,-2) = (-2,3) = 1$

$\Rightarrow 747^{-1} = 3 \Rightarrow \boxed{d = 3}$ – cheia privată

$N = 30$, $n = 1189$, $\varphi(n) = 1120$, $e = 747$, $d = 3$, BFCAFNBIW

BFCAFNBiW = 1520 5(13) 18(22)

$j = 3$, $l = 4$

- $BFC = 152_? = 1 \cdot 30^2 + 5 \cdot 30^1 + 2 \cdot 30^0 = 900 + 150 + 2 = 1052 = c$

  $m' = c^d \pmod{n} = 1052^3 \pmod{1189} = 454$

- $AFN = 05(13) = 0 \cdot 30^2 + 5 \cdot 30^1 + 13 \cdot 30^0 = 0 + 150 + 13 = 163 = c$

  $m' = 163^3 \pmod{1189} = 409$

- $BiW = 18(22) = 1 \cdot 30^2 + 8 \cdot 30^1 + 22 \cdot 30^0 = 900 + 240 + 22 = 1162$

  $m' = 1162^3 \pmod{1189} = 530$

$454 = 0 \cdot 30^2 + 15 \cdot 30^1 + 4 \cdot 30^0 = 0(15)4 = APE$
$409 = 0 \cdot 30^2 + 13 \cdot 30^1 + 19 \cdot 30^0 = 0(13)(19) = ANT$
$530 = 0 \cdot 30^2 + 17 \cdot 30^1 + 20 \cdot 30^0 = 0(17)(20) = ARU$

} PENTRU

1. Ana și Bob folosesc RSA. Ana are cheia secretă (n = 12827, d = 2291). Determinați cheia sa publică și criptați textul **IERI** dacă lungimea blocurilor în clar este 2 și lungimea blocurilor criptate este 3.

$K_d (n = 12827, d = 2291)$
$j = 2, \ell = 3$

a) $K_e(n, e)$
b) criptați IERI

$d \cdot e \equiv 1 \pmod{\varphi(n)}$
$\varphi(n) = (p-1)(q-1)$
$n = p \cdot q$
$n = 12827$ TE⇒

$\sqrt{12827}$ | 113 ⇒ $\lfloor \sqrt{12827} \rfloor = 113$
1
= 28 | $21 \cdot 1 = 21$
21 | $223 \cdot 3 = 669$
= 727
669
58

$t = 114 \Rightarrow 114^2 - 12827 = 169 = 13^2 \Rightarrow s = 13 \Rightarrow n = (t-s)(t+s) = (114-13)(114+13) =$
$= \underbrace{101}_{p} \cdot \underbrace{127}_{q}$

$\varphi(n) = 100 \cdot 126 = 12600$
$d = 2291$
$\Rightarrow 2291 \cdot e \equiv 1 \pmod{12600} \Leftrightarrow$

$\Leftrightarrow e \equiv 2291^{-1} \pmod{12600} = 11$

$12600 = 2291 \cdot 5 + 1145 \Rightarrow x_{1145} = x_{12600} - 5 \cdot x_{2291} = (1,0) - (0,5) =$
$= (1, -5)$
$2291 = 1145 \cdot 2 + 1 \Rightarrow x_1 = x_{2291} - 2 \cdot x_{1145} = (0,1) - (2,-10) =$
$= (-2, \underbrace{11}_{e})$

$\Rightarrow K_e (n = 12827, e = 11)$

$IERI = \underbrace{84}\underbrace{(17)}\underbrace{8}, N = 30$

- $IE = 8 \cdot 30^1 + 4 \cdot 30^0 = 240 + 4 = 244 = m \Rightarrow c = m^e \pmod{n} =$
$= 244^{11} \pmod{12827} = 4851 = 5 \cdot 30^2 + 11 \cdot 30^1 + 21 \cdot 30^0 \Rightarrow 5(11)(21) = FLV$
- $RI = 17 \cdot 30^1 + 8 \cdot 30^0 = 510 + 8 = 518 = m \Rightarrow c = 518^{11} \pmod{12827} =$
$= 7595 = 8 \cdot 30^2 + 13 \cdot 30^1 + 5 \cdot 30^0 = 8(13)5 = INF$