TEMA 7

(ex. 5) RSA

cheia publică $K_e = (n=1189, e=747)$

a) cheia privată?

b) $N^j \le n \le N^{j+1}$, lungimea blocurilor $l = j+1$

N - lungime alfabet ; BFCAFNBiW.

Rezolvare

a) $Kd_A = (d_A, n_A)$

$d = e^{-1} \pmod{\varphi(n)}$

$n = p \cdot q = 1189 = 29 \cdot 41$

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

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

$n = 35^2 - 6^2 = (35-6)(35+6) = 29 \cdot 41$

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

$d = e^{-1} \pmod{1120} = 747^{-1} \pmod{1120}$

$X_{1120} = (1,0)$

$X_{747} = (0,1)$

$1120 : 747 = 1$, r. $373 \Rightarrow X_{373} = X_{1120} - X_{747} = (1,0) - (0,1) = (1,-1)$

$747 : 373 = 2$, r. $1 \Rightarrow X_1 = X_{747} - 2 \cdot X_{373} = (0,1) - (2,-2) = (-2,3)$

$\Rightarrow e^{-1} \pmod{1120} = 3 \Rightarrow \boxed{d=3}$ (cheia privată)

b) $N=30$.

$30^j \leq 1189 \leq 30^{j+1}$

$j=2 \Rightarrow 900 \leq 1189 \leq 27000$

deci $\underline{l=3}$

împărțim textul în blocuri de lungime 3

$\overbrace{BFC}\overbrace{AFM}\overbrace{BIW}$

$BFC = (1)(5)(2) = 2\cdot 30^0 + 5\cdot 30 + 30^2 = 2+150+900 = 1052$

$AFM = (0)(5)(13) = 13 + 5\cdot 30 = 163$

$BIW = (2)(8)(22) = 22 + 8\cdot 30 + 2\cdot 30^2 = 2062$