Tema 7

(13)

a) $p \cdot q = 23 \cdot 17 = 391 \Rightarrow (n, e) = (391, 3)$

$\varphi(n) = 22 \cdot 16 = 352$

$e \cdot d \equiv 1 \pmod{352}$ (d - cheia de criptare)

$\Rightarrow d \equiv 3^{-1} \Rightarrow d = 117$

HELP_ME!

$c \equiv m^e \pmod{n}$:

H $\Rightarrow 7^3 \equiv 343 \pmod{391}$

E $\Rightarrow 4^3 \equiv 64 \pmod{391}$

L $\Rightarrow 11^3 \equiv 138$

P $\Rightarrow 15^3 \equiv 252$

_ $\Rightarrow 28^3 \equiv 60$

M $\Rightarrow 12^3 \equiv 164$

E $\Rightarrow 4^3 \equiv 64$

! $\Rightarrow 22^3 \equiv 135$

$\Rightarrow$ Mesajul: 343, 64, 138, 252, 60, 164, 64, 135.

b) EB MM AA F OMML! EB AI HI

EB MM AA F OM ML ! EB AI HI

4,1 12,12 0,0 5,26 14,12 12,11 27 4,1 0,8 7,8.

Se var calcula:

E → 4 ^{117} mod 391

B → 1 ^{117} mod 391

M → 12 ^{117}

A → 0 ^{117}

F → 5 ^{117}

O → 14 ^{117}

L → 11 ^{117}

! → 27 ^{117}

I → 8 ^{117}

H → 7 ^{117}

mod 391

Iar conform ~~poza~~ pergr. de la seminar =>

=> în clar: HELP_ME.