14

Tema 7
Valachi Emilia, M532

Iulia și Andrei folosesc criptosistemul RSA.

Iulia are $K_{e_I} = (n_I = 9991,\ e_I = 3917)$

a) Determinați cheia privată a Iuliei.

$9991 = p \cdot q \Rightarrow \varphi(9991) = (p-1)(q-1)$

$p = 97,\ q = 103$

$\varphi(9991) = (97-1)(103-1) = 9792$

$d_A e_A \equiv 1 \pmod{\varphi(n)} \Rightarrow d = 3917^{-1} \pmod{9792}$

Euclid:

$3917 \cdot 2 + 1958 = 9792$

$3917 = 1958 \cdot 2 + 1$

$1958 = 1958 + 0$

$1 = 3917 - 2 \cdot 1958$

$1 = 3917 - 2 \cdot (9792 - 2 \cdot 3917)$

$1 = 3917 - 2 \cdot 9792 + 4 \cdot 3917$

$1 = (5) \cdot 3917 - 2 \cdot 9792 \Rightarrow Kd_I = (9991, 5)$

b) Decriptați mesajul $\overline{BMMA\_X}^{c}$ primit de Iulia, dacă lungimea blocurilor în clar este 2 și criptate - 3.

BMM → 1 12 7

A_X → 0 26 23

$BMX = 1 \cdot 30^2 + 12 \cdot 30 + 7 = \overline{1267}^{m_1} \Rightarrow m_1' = 1267^{5} \pmod{9991}$

$= 404 \pmod{10?}$

$\rightarrow 14 \rightarrow O$

$A\_X = 26 \cdot 30 + 23 = \overline{803}^{m_2} \Rightarrow m_2' =$

$= 803^{5} \pmod{9991} = 570 \pmod{10?}$

$\rightarrow 19 \rightarrow T$