KRIPTOGRAFIJA

Zadaća 5.213 *X*

Rok za podizanje zadaće je od 16.05.2007. do (uključivo) 23.05.2007. Rok za predaju ove zadaće je 30.05.2007

1. Odaberite dva različita četveroznamenkasta prosta broja p i q. Neka je $n = p \cdot q$. Odaberite peteroznamenkasti broj e koji je relativno prost sa $\varphi(n)$. Šifrirajte otvoreni tekst
$$x = 659503$$
pomoću RSA kriptosustava s javnim ključem (n, e). Odredite pripadni tajni ključ d.

2. Alice je poslala istu poruku m nekolicini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA sustav sa javnim eksponentom $e = 3$.
Za zadane
$$\begin{aligned} n_1 &= 5183, & c_1 &= 1049, \\ n_2 &= 6557, & c_2 &= 3746, \\ n_3 &= 12317, & c_3 &= 4830, \end{aligned}$$
pomozite Evi da otkrije poruku m.

3. Neka je (e, n) Bobov javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{\sqrt[4]{n}}{3}$. Odredite d (Bobov tajni ključ) i pomoću njega dešifrirajte poruku c koju je Alice poslala Bobu.
Ulazni podaci su
$$\begin{aligned} e &= 1246848097643993, \\ n &= 2514232617180497, \\ c &= 661556259504829. \end{aligned}$$

Napomene:
1. zadatak – (modularno) potenciranje treba napraviti na ruke.
2. i 3. zadatak nije dozvoljeno rješavati faktorizacijom.
23.05.2007. nema ni predavanja ni vježbi.