KRIPTOGRAFIJA

Zadaća 5.79 *Prezime Ime*

Rok za podizanje zadaće je od 21.05.2004. do (uključivo) 28.05.2004. Rok za predaju ove zadaće je 04.06.2004

2. i 3. zadatak nije dozvoljeno rješavati faktorizacijom.

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

   $$x = 762236$$

   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

   $$\begin{aligned} n_1 &= 5293, & c_1 &= 5279, \\ n_2 &= 10379, & c_2 &= 2944, \\ n_3 &= 13843, & c_3 &= 7554, \end{aligned}$$

   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

   $$\begin{aligned} e &= 1913532288587, \\ n &= 16134564376001, \\ c &= 6012045904403. \end{aligned}$$

4. Nađite dva pseudoprosta broja u bazi $b = 89$.