KRIPTOGRAFIJA

Zadaća 5.1

Rok za podizanje zadaće je od 23.05.2003. do (uključivo) 30.05.2003. Rok za predaju ove zadaće je 06.06.2003.

U 2. i 3. zadatku nije dozvoljeno rješavanje korištenjem faktorizacije brojeva n_1, n_2, n_3, odnosno n.

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

   $$x = 120343$$

   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

   $$\begin{aligned} n_1 &= 1457 & c_1 &= 281 \\ n_2 &= 2923 & c_2 &= 270 \\ n_3 &= 1537 & c_3 &= 1343 \end{aligned}$$

   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

   $$\begin{aligned} e &= 13155587841637 \\ n &= 21303975357773 \\ c &= 9083132718469. \end{aligned}$$

4. Nađite dva pseudoprosta broja u bazi $b = 47$.