KRIPTOGRAFIJA

Zadaća 4.176 *X*

Rok za podizanje zadaće je od 19.05.2006. do (uključivo) 26.05.2006. Rok za predaju ove zadaće je 02.06.2005

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

   $$x = 866096$$

   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

   $$\begin{aligned} n_1 &= 5767, & c_1 &= 1384, \\ n_2 &= 9797, & c_2 &= 3332, \\ n_3 &= 11663, & c_3 &= 4446, \end{aligned}$$

   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

   $$\begin{aligned} e &= 322380640497533, \\ n &= 608602420657423, \\ c &= 304243444482031. \end{aligned}$$

4. Nađite dva pseudoprosta broja u bazi $b = 37$.