Kriptografija i sigurnost mreža

završni ispit - grupa A

16.1.2015.

1. 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 kriptosustav s javnim eksponentom $e = 3$. Za zadane

$$\begin{aligned} n_1 &= 371, \qquad c_1 = 34, \\ n_2 &= 403, \qquad c_2 = 27, \\ n_3 &= 493, \qquad c_3 = 190. \end{aligned}$$

   pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

2. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (5561, 67, 83),$$

   dešifrirajte šifrat $y = 3241$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

3. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (3, 7, 11, 27, 53, 111, 219, 441), \quad p = 929, \quad a = 131, \\ t &= (393, 917, 512, 750, 440, 606, 819, 173). \end{aligned}$$

   Dešifrirajte šifrat $y = 2280$.

4. Je li broj 185

   a) pseudoprost u bazi 6,

   b) jaki pseudoprost u bazi 6?

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 647239$ (poznato je da je n produkt dva "bliska" prosta broja).

Dozvoljeno je korištenje džepnog kalkulatora, te dva papira s formulama.
Kalkulatori se mogu koristiti za standardne operacije, ali nije dozvoljeno korištenje gotovih funkcija za modularno potenciranje, modularni inverz, rješavanje linearnih kongruencija i sustava linearnih kongruencija, faktorizaciju i sl.

Rezultati: petak, 23.1.2015. u 12 sati. Andrej Dujella