Kriptografija i sigurnost mreža

završni ispit - grupa A

15.12.2011.

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

$$\begin{aligned} n_1 &= 371, \qquad c_1 = 349, \\ n_2 &= 403, \qquad c_2 = 312, \\ n_3 &= 551, \qquad c_3 = 236. \end{aligned}$$

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

2. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (3713, 47, 79),$$

   dešifrirajte šifrat $y = 3020$. 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

$$\begin{aligned} v &= (3, 7, 12, 31, 58, 121, 238, 490), \quad p = 967, \quad a = 127, \\ t &= (381, 889, 557, 69, 597, 862, 249, 342). \end{aligned}$$

   Dešifrirajte šifrat $y = 1389$.

4. Je li broj 533

   a) pseudoprost u bazi 40,

   b) Eulerov pseudoprost u bazi 40,

   c) jaki pseudoprost u bazi 40?

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 704203$ (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: četvrtak, 22.12.2011. u 12 sati. Andrej Dujella