Kriptografija i sigurnost mreža

završni ispit - grupa A

18.1.2016.

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

$$\begin{aligned} n_1 &= 413, \qquad c_1 = 274, \\ n_2 &= 481, \qquad c_2 = 177, \\ n_3 &= 589, \qquad c_3 = 407. \end{aligned}$$

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

2. Neka je u ElGamalovom kriptosustavu $p = 1229$, $\alpha = 2$, $a = 37$. Dešifrirajte šifrat $(388, 225)$.

3. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 7, 11, 25, 51, 102, 207, 419), \ \ p = 907, \ \ a = 137, \\ t &= (274, 52, 600, 704, 638, 369, 242, 262). \end{aligned}$$

   Dešifrirajte šifrat $y = 1563$.

4. Je li broj 341

   a) pseudoprost u bazi 2,

   b) jaki pseudoprost u bazi 2?

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 737419$ (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: ponedjeljak, 25.1.2016. u 14 sati.

Andrej Dujella