Kriptografija i sigurnost mreža

završni ispit - grupa A

24.1.2014.

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

$$\begin{aligned} n_1 &= 377, \qquad c_1 = 285, \\ n_2 &= 407, \qquad c_2 = 214, \\ n_3 &= 589, \qquad c_3 = 202. \end{aligned}$$

   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 $y = 2311$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

3. Neka je u ElGamalovom kriptosustavu $p = 1117$, $\alpha = 2$, $a = 77$. Dešifrirajte šifrat $(470, 472)$.

4. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 7, 12, 29, 56, 119, 241, 487), \ \ p = 977, \ \ a = 257, \\ t &= (514, 822, 153, 614, 714, 296, 386, 103). \end{aligned}$$

   Dešifrirajte šifrat $y = 1985$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 579749$ (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: srijeda, 29.1.2014. u 12 sati. Andrej Dujella