Kriptografija i sigurnost mreža

završni ispit - grupa A

14.12.2012.

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

$$\begin{aligned} n_1 &= 437, \qquad c_1 = 30, \\ n_2 &= 481, \qquad c_2 = 408, \\ n_3 &= 527, \qquad c_3 = 314. \end{aligned}$$

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

2. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (3337, 47, 71),$$

   dešifrirajte šifrat $y = 2194$. 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 $p = 1619$, $\alpha = 2$, $a = 39$. Dešifrirajte šifrat $(720, 702)$.

4. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 7, 11, 27, 58, 117, 238, 475), \ \ p = 971, \ \ a = 127, \\ t &= (254, 889, 426, 516, 569, 294, 125, 123). \end{aligned}$$

   Dešifrirajte šifrat $y = 2097$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 627401$ (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, 19.12.2012. u 10 sati.

Andrej Dujella