Kriptografija i sigurnost mreža

završni ispit

28.1.2022.

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

$$\begin{aligned} n_1 &= 437, \qquad c_1 = 227, \\ n_2 &= 473, \qquad c_2 = 59, \\ n_3 &= 527, \qquad c_3 = 411. \end{aligned}$$

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

2. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (5609, 71, 79),$$

   dešifrirajte šifrat $y = 1589$. 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

$$\begin{aligned} v &= (4, 5, 17, 29, 58, 120, 241, 477), \quad p = 967, \quad a = 786, \\ t &= (243, 62, 791, 553, 139, 521, 861, 693). \end{aligned}$$

   Dešifrirajte šifrat $y = 3141$.

4. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 6757747$ (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.

Andrej Dujella