Kriptografija i sigurnost mreža

završni ispit – grupa A

22.1.2025.

1. Neka je $(n, e) = (18976663, 4462993)$ javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{1}{3}\sqrt[4]{n}$. Odredite d pomoću Wienerovog napada.

2. 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

$$\begin{aligned} n_1 &= 437, & c_1 &= 419, \\ n_2 &= 473, & c_2 &= 426, \\ n_3 &= 527, & c_3 &= 349. \end{aligned}$$

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

3. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (4757, 67, 71),$$

   dešifrirajte šifrat $y = 1421$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

4. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (1, 6, 11, 20, 39, 85, 169, 333), \quad p = 673, \quad a = 618, \\ t &= (618, 343, 68, 246, 547, 36, 127, 529). \end{aligned}$$

   Dešifrirajte šifrat $y = 1798$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 6898093$ (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