Kriptografija i sigurnost mreža

završni ispit - grupa A

25.1.2023.

1. Neka je $(n, e) = (18597437, 3280337)$ 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

$$\begin{aligned} n_1 &= 437, \qquad & c_1 &= 164, \\ n_2 &= 473, \qquad & c_2 &= 293, \\ n_3 &= 527, \qquad & c_3 &= 461. \end{aligned}$$

   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 $y = 1387$. 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

$$\begin{aligned} v &= (4, 8, 20, 34, 70, 142, 282, 563), \quad p = 1129, \quad a = 832, \\ t &= (1070, 1011, 834, 63, 661, 728, 921, 1010). \end{aligned}$$

   Dešifrirajte šifrat $y = 4303$.

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: petak, 27.1.2023. u 13 sati. Andrej Dujella