Kriptografija i sigurnost mreža

završni ispit - grupa A

23.1.2018.

1. Neka je $(n, e) = (18603427, 5468993)$ 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

$$\begin{aligned} n_1 &= 371, \qquad & c_1 &= 148, \\ n_2 &= 437, \qquad & c_2 &= 198, \\ n_3 &= 629, \qquad & c_3 &= 195. \end{aligned}$$

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

3. Neka je u ElGamalovom kriptosustavu $p = 509$, $\alpha = 2$, $a = 47$. Dešifrirajte šifrat $(60, 444)$.

4. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (1, 6, 9, 19, 43, 91, 185, 383), \quad p = 911, \quad a = 239, \\ t &= (239, 523, 329, 897, 256, 796, 487, 437). \end{aligned}$$

   Dešifrirajte šifrat $y = 2150$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 1437209$ (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, 31.1.2018. u 14 sati. Andrej Dujella