Kriptografija i sigurnost mreža

završni ispit - grupa A

27.1.2017.

1. Neka je $(n, e) = (20293993, 10676179)$ 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

$$\begin{aligned} n_1 &= 413, \qquad & c_1 &= 8, \\ n_2 &= 437, \qquad & c_2 &= 151, \\ n_3 &= 629, \qquad & c_3 &= 117. \end{aligned}$$

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

3. Neka je u ElGamalovom kriptosustavu $p = 1229$, $\alpha = 2$, $a = 47$. Dešifrirajte šifrat $(690, 940)$.

4. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 6, 11, 23, 49, 101, 205, 413), \ \ p = 907, \ \ a = 139, \\ t &= (278, 834, 622, 476, 462, 434, 378, 266). \end{aligned}$$

   Dešifrirajte šifrat $y = 2176$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 860677$ (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: petak, 3.2.2017. u 12 sati.

Andrej Dujella