

Kriptografija i sigurnost mreža

završni ispit - grupa A

22.1.2019.

1. Neka je $(n, e) = (18576959, 13106897)$ 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

$$\begin{aligned}n_1 &= 427, & c_1 &= 64, \\n_2 &= 437, & c_2 &= 286, \\n_3 &= 527, & c_3 &= 500.\end{aligned}$$

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

3. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (5293, 67, 79),$$

dešifrirajte šifrat $y = 2593$. 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

$$\begin{aligned}v &= (1, 5, 8, 19, 39, 85, 175, 363), & p &= 853, & a &= 241, \\t &= (241, 352, 222, 314, 16, 13, 378, 477).\end{aligned}$$

Dešifrirajte šifrat $y = 949$.

5. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 6317137$ (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, 30.1.2019. u 13 sati.

Andrej Dujella