

Kriptografija i sigurnost mreža

završni ispit – grupa A

24.1.2024.

1. 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

$$\begin{aligned}n_1 &= 437, & c_1 &= 201, \\n_2 &= 473, & c_2 &= 388, \\n_3 &= 527, & c_3 &= 464.\end{aligned}$$

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

2. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (5561, 67, 83),$$

dešifrirajte šifrat $y = 1605$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

3. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned}v &= (3, 4, 14, 26, 51, 104, 209, 412), & p &= 827, & a &= 639, \\t &= (263, 75, 676, 74, 336, 296, 404, 282).\end{aligned}$$

Dešifrirajte šifrat $y = 1063$.

4. Fermatovom metodom faktorizacije rastavite na proste faktore broj $n = 6830911$ (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