Diskretna matematika

ponovljeni završni ispit

6.2.2009.

1. U polju $\mathbb{F}_{2^8}$, definiranom kao $\mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$, odredite produkt polinoma
$$x^6+x^5+x^3+x^2+1 \quad \text{i} \quad x^7+x^4+x^2+x+1.$$

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
$$\begin{aligned} n_1 &= 403, & c_1 &= 116,\\ n_2 &= 407, & c_2 &= 393,\\ n_3 &= 551, & c_3 &= 210. \end{aligned}$$
pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

3. Neka je $(n,e) = (32311427, 22100011)$ Bobov javni RSA ključ. Poznato je da tajni eksponent d zadovoljava nejednakost $d < \frac{1}{3}\sqrt[4]{n}$. Odredite d (Bobov tajni RSA ključ) i i pomoću njega dešifrirajte šifrat $y = 843$ koji je Alice poslala Bobu.

4. U Rabinovu kriptosustavu s parametrima
$$(n,p,q) = (3713, 47, 79),$$
dešifrirajte šifrat $y = 1521$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

5. Zadan je Merkle-Hellmanov kriptosustav s parametrima
$$\begin{aligned} v &= (3,5,11,27,53,109,209,425), \quad p = 853, \quad a = 127,\\ t &= (381,635,544,17,760,195,100,236). \end{aligned}$$
Dešifrirajte šifrat $y = 1627$.

6. Odredite sve proste brojeve p takve da je Legendreov simbol $\left(\frac{7}{p}\right) = 1$.

7. Neka je $(\mathbb{R}^*, \cdot)$ multiplikativna grupa realnih brojeva različitih od nule, a $X = \mathbb{R}^* \times \mathbb{R}$. Na X definiramo binarnu operaciju $\bullet$ sa
$$(a,b) \bullet (a',b') = (aa', ab'+b).$$
Dokažite da je $(X, \bullet)$ grupa. Je li ta grupa Abelova?

Dozvoljeno je korištenje džepnog kalkulatora.
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, razvoj u verižni razlomak i sl.

Andrej Dujella i Marcel Maretić