Diskretna matematika

Zadaci za vježbu - treći ciklus 2009/2010

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

   a) $x^7+x^5+x^4+x$ i x^7+x^6+x;

   b) $x^4+x^3+x^2$ i $x^6+x^4+x^3+1$.

2. Izračunajte:

   a) $(\mathtt{B6}x^3+\mathtt{AE}x^2+\mathtt{A8}x+\mathtt{BF})\otimes(\mathtt{FA}x^3+\mathtt{0B}x^2+\mathtt{79}x+\mathtt{7C})$;

   b) $(\mathtt{49}x^3+\mathtt{20}x^2+\mathtt{9A}x+\mathtt{24})\otimes(\mathtt{F0}x^3+\mathtt{8F}x^2+\mathtt{93}x+\mathtt{60})$.

3. U RSA kriptosustavu s javnim ključem (n,e), gdje je $n=86267=281\cdot 307$ i $e=65537$, šifrirajte otvoreni tekst

   $$x=1245.$$

   Odredite pripadni tajni ključ d.

4. Otvoreni je tekst na hrvatskom jeziku šifriran pomoću RSA kriptosustava, čiji je javni ključ $(n,e)=(30967,17)$. Najprije su slovima pridružene odgovarajuće brojevne vrijednosti: A = 0, B = 1, C = 2, Č = 3, ... , Z = 28, Ž = 29. Potom su tri po tri susjedna slova otvorenog teksta "kodirana" kao elementi od $\mathbb{Z}_n$, kao što pokazuju ovi primjeri:

   $$DAN = 5\cdot 30^2+0\cdot 30+18 = 4518, \quad PUT = 21\cdot 30^2+26\cdot 30+25 = 19705.$$

   Konačno su ovako dobiveni elementi od $\mathbb{Z}_n$ šifrirani pomoću RSA kriptosustava s gore navedenim parametrima n i e.

   Faktorizirajte broj n (poznato je da je produkt dvaju "bliskih" prostih brojeva), te dešifrirajte šifrat

   $$23144, \quad 14420, \quad 19603, \quad 27580.$$

5. 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

$$\begin{aligned} n_1 &= 407, \qquad c_1 = 356, \\ n_2 &= 533, \qquad c_2 = 281, \\ n_3 &= 551, \qquad c_3 = 468. \end{aligned}$$

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

6. Neka je $(n, e) = (7478291, 4395713)$ 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).

7. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (3713, 47, 79),$$

dešifrirajte šifrat $y = 1512$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

8. Neka je u Diffie-Hellmanovom protokolu $G = \mathbb{Z}_p^*$, $p = 87671$, te $g = 2$, $a = 1234$, $b = 4321$. Odredite ključ $K = g^{ab}$.

9. Neka je u ElGamalovom kriptosustavu $p = 1777$, $\alpha = 6$, $a = 1009$.

   a) Šifrirajte otvoreni tekst $x = 1483$, uz pretpostavku da je jednokratni ključ $k = 701$.

   b) Dešifrirajte šifrat $(1664, 1031)$.

10. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 5, 13, 27, 55, 119, 223), \ \ p = 449, \ \ a = 307, \\ t &= (165, 188, 399, 207, 272, 164, 213). \end{aligned}$$

Dešifrirajte šifrat $y = 1021$.

11. Zadan je Merkle-Hellmanov kriptosustav s parametrima

$$\begin{aligned} v &= (2, 5, 11, 27, 53, 109, 211, 423), \ \ p = 853, \ \ a = 127, \\ t &= (254, 635, 544, 17, 760, 195, 354, 835). \end{aligned}$$

Dešifrirajte šifrat $y = 1607$.