Programiranje II. Konsultacije za završni ispit. Zadaci iz Algoritmi u teoriji brojeva i u kriptografiji. 8–16 {9 zadataka}

Postavke zadataka

(10) Riješiti sistem jednačina: $x \bmod 7 = 2$, $x \bmod 15 = 3$ po nepoznatoj x $(0 \le x \le 104)$.

(11) Naći bar jedno rješenje jednačine $7x - 6y = 16$, gdje se nepoznate x i y traže u skupu cijelih brojeva, ako rješenje postoji. Može se primijeniti uopšteni Euklidov algoritam.

(12) Razmotrimo RSA kriptografski sistem: $p = 5$, $q = 7$, $n = pq = 35$, $\varphi(n) = (p-1)(q-1) = 24$, $e = 5$, $d = 5$. Neka poruka glasi $M = 20$. Izračunati kodirani oblik poruke $C = M^e \bmod n$. Zatim izračunati $C^d \bmod n$ (uvjeriti se da izlazi M). Ponoviti isti račun za još neko M $(1 < M < n)$.

(13) Razmotrimo metodu kvadratnog ostatka: $p = 7$, $q = 11$, $n = pq = 77$. Neka poruka glasi $x = 15$ $(1 \le x \le n-1)$. Izračunati $y = x^2 \bmod n$, tj. izvršiti enkripciju. Da bismo se uvjerili da su formule za dekripciju pravilne, izračunati $y_1 = (y \bmod p)^{(p+1)/4} \bmod p$ i $y_2 = (y \bmod q)^{(q+1)/4} \bmod q$ i zatim vidjeti da važi $x \equiv \pm y_1 \pmod p$, $x \equiv \pm y_2 \pmod q$.

(15) Ispitivanje primalnosti (da li je dati broj n prost). Razmotrimo Millerov postupak i $n = 91$. Za $b = 2$, da li važi $b^{n-1} \bmod n = 1$. Drugim riječima, uzimajući u obzir da je dati broj n složen, da li je dati broj pseudo–prost u bazi $b = 2$. Isto pitanje u slučaju baze $b = 3$.

(16) Ispitivanje primalnosti (da li je dati broj n prost). Primijeniti Millerov postupak (test) na broj $n = 91$ po četiri baze ($b = 2$, $b = 3$, $b = 5$ i $b = 7$). Prolazi li n test?

Rješenja zadataka

(8) NZD$(2420, 196)$.

(9) $\pi(x)$, $x = 1000$, $x = 10000$.

(10) $x \bmod 7 = 2$, $x \bmod 15 = 3$, $0 \le x \le 104$.

$x = 7a + 2 \quad x = 15b + 3$

$7a + 2 = 15b + 3$

$7a - 15b = 1 \quad \text{NZD}(7, 15) = 1$

(smanjivanje koeficijenata, da se svede na jedinicu)

$7(a - 2b) - b = 1 \quad a - 2b = c$

$7c - b = 1$

$b = 7c - 1$

c=0 b=−1 a=2b+c=−2 x=−12 x=−12

c=1 b=6 a=2b+c=13 x=91+2 x=90+3

Odgovor: $x = 93$.

(11) $7x - 6y = 16$.

NZD$(7, 6)$=1, $1|16$, tako da rješenje postoji.

$x + (6x - 6y) = 16 \quad z = x - y$

$x + 6z = 16$

$x = 16 - 6z$

$z = -1 \quad x = 22 \quad y = 23$

$z = 0 \quad x = 16 \quad y = 16$

$z = 1 \quad x = 10 \quad y = 9$

$(x, y) = \ldots, (4, 2), (10, 9), (16, 16), (22, 23), \ldots$

Mogući odgovor: $x = 4$, $y = 2$.

(12) $e = 5 \quad d = 5 \quad M = 20 \quad n = 35$.

$C = M^e \bmod n = 20^5 \bmod 35 =$

$(400 \bmod 35)^2 \cdot 20 \bmod 35 =$

$(15^2 \cdot 20) \bmod 35 = (225 \cdot 20) \bmod 35 =$

$(15 \cdot 20) \bmod 35 = 300 \bmod 35 = 20$

$C^d \bmod n = 20^5 \bmod 35 = 20$

Da bi se izbjeglo slučajno poklapanje M i C do koga je došlo: $M = 19$

$C = M^e \bmod n = 19^5 \bmod 35 =$

$361 \cdot 361 \cdot 19 \bmod 35 = 11 \cdot 11 \cdot 19 \bmod 35 =$

$121 \cdot 19 \bmod 35 = 16 \cdot 19 \bmod 35 =$

$304 \bmod 35 = 24$

$C^d \bmod n = 24^5 \bmod 35 =$

$576 \cdot 576 \cdot 24 \bmod 35 = 16 \cdot 16 \cdot 24 \bmod 35 =$

$256 \cdot 24 \bmod 35 = 11 \cdot 24 \bmod 35 =$

$264 \bmod 35 = 19$

Vidimo da je zaista $M = C^d \bmod n$.

Pokušavamo da izbjegnemo slučajno poklapanje e i d do koga je došlo

$\varphi(n) = 24, \quad ed \equiv 1 \pmod{\varphi(n)}$

$e =$	1	5	7	11	13	17	19	23
$d =$	1	5	7	11	13	17	19	23

vidimo da ne može da se izbjegne (sa datim n)

Uzmimo sve brojeve nove u postavci zadatka
$p = 5$ prost $\quad q = 11$ prost
$n = pq = 55 \quad \varphi(n) = (p-1)(q-1) = 40$
$e = 3, \quad d = 27$ (još bi moglo i $e = 7, \quad d = 23$)
$M = 8$

$C = M^e \bmod n = 8^3 \bmod 55 =$
$512 \bmod 55 = 17$

$C^d \bmod n = 17^{27} \bmod 55 =$
$(289 \cdot 17)^9 \bmod 55 = (14 \cdot 17)^9 \bmod 55 =$
$238^9 \bmod 55 = 18^9 \bmod 55 =$
$(324 \cdot 18)^3 \bmod 55 = (49 \cdot 18)^3 \bmod 55 =$
$((-6) \cdot 18)^3 \bmod 55 = (-108)^3 \bmod 55 =$
$2^3 \bmod 55 = 8 \bmod 55 = 8$

Vidimo da je zaista $M = C^d \bmod n$

M – poruka u jasnom obliku, C – kodirana poruka, $C = M^e \bmod n$ – formula za enkripciju, $M = C^d \bmod n$ – formula za dekripciju (ovo je RSA sistem)

(13) Rabinov sistem ili sistem kvadratnog ostatka, x – poruka u jasnom obliku, y – kodirana poruka, $y = x^2 \bmod n$ – formula za enkripciju, formule za dekripciju:
$y_1 = y^{(p+1)/4} \bmod p,$
$y_2 = y^{(q+1)/4} \bmod q$

$$\begin{cases} x \equiv \pm y_1 \,(\mathrm{mod}\, p) \\ x \equiv \pm y_2 \,(\mathrm{mod}\, q) \end{cases}$$

Dato je: $p = 7$ prost, $p \equiv 3 \,(\mathrm{mod}\, 4)$,
$q = 11$ prost, $q \equiv 3 \,(\mathrm{mod}\, 4)$,
$n = pq = 77, \quad x = 15.$

Vršimo enkripciju:

$y = x^2 \bmod n = 225 \bmod 77 = 71$

Uvjeravamo se da su formule za dekripciju pravilne:

$y_1 = (y \bmod p)^{(p+1)/4} \bmod p =$
$(71 \bmod 7)^2 \bmod 7 = 1,$

$y_2 = (y \bmod q)^{(q+1)/4} \bmod q =$
$(71 \bmod 11)^3 \bmod 11 = 5^3 \bmod 11 = 4$

$$\begin{cases} x \equiv \pm y_1 \,(\mathrm{mod}\, p) \\ x \equiv \pm y_2 \,(\mathrm{mod}\, q) \end{cases}$$

$$\begin{cases} 15 \equiv \pm 1 \,(\mathrm{mod}\, 7) \\ 15 \equiv \pm 4 \,(\mathrm{mod}\, 11) \end{cases} \quad \begin{cases} 15 \equiv 1 \,(\mathrm{mod}\, 7) \\ 15 \equiv 4 \,(\mathrm{mod}\, 11) \end{cases}$$

(14) Rabin, enkripcija i dekripcija.

(15) Millerov, $n = 91$ (dati broj je složen).

$b = 2$

Treba izračunati $y = b^{n-1} \bmod n$ i vidjeti da li je $y = 1$

$y = b^{n-1} \bmod n = 2^{90} \bmod 91 =$
$(2^{13})^7 : 2 \bmod 91 = 8192^7 : 2 \bmod 91 =$
$2^7 : 2 \bmod 91 = 2^6 \bmod 91 = 64 \bmod 91 = 64$

$y = 64 \quad y \neq 1$

$b = 3$

Treba izračunati $y = b^{n-1} \bmod n$ i vidjeti da li je $y = 1$

$y = b^{n-1} \bmod n = 3^{90} \bmod 91 =$
$243^{18} \bmod 91 = 61^{18} \bmod 91 =$
$3721^9 \bmod 91 = (-10)^9 \bmod 91 =$
$100^4(-10) \bmod 91 = 9^4(-10) \bmod 91 =$
$81^2(-10) \bmod 91 = (-10)^2(-10) \bmod 91 =$
$100(-10) \bmod 91 = 9(-10) \bmod 91 =$
$(-90) \bmod 91 = 1$

Odgovor:

$$\begin{cases} n = 91 \text{ nije pseudo–prost u bazi } b = 2 \\ n = 91 \text{ jeste pseudo–prost u bazi } b = 3 \end{cases}$$

(16) Millerov $\quad b = 2, 3, 5, 7 \quad n = 91.$

$y = b^{n-1} \bmod n$ (da li je $y = 1$)
$y = 2^{90} \bmod 91 = \ldots = 64 \neq 1$
$y = 3^{90} \bmod 91 = \ldots = 1$
$y = 5^{90} \bmod 91 = \ldots \neq 1$
$y = 7^{90} \bmod 91 = \ldots \neq 1$

$$\begin{cases} n \text{ nije pseudo–prost u bazi } b = 2 \\ n \text{ jeste pseudo–prost u bazi } b = 3 \\ n \text{ nije pseudo–prost u bazi } b = 5 \\ n \text{ nije pseudo–prost u bazi } b = 7 \end{cases} \Rightarrow$$

n ne prolazi test po 4 baze $\Rightarrow$
n je (sigurno) složen

Odgovor: broj $n = 91$ ne prolazi Millerov test po bazama $b = 2$, $b = 3$, $b = 5$, $b = 7$.

Da izložimo opštu šemu Millerovog testa:

na bar jednom mjestu piše "nije" $\Rightarrow$ ne prolazi test $\Rightarrow$ broj n je sigurno složen,

na svim mjestima piše "jeste" $\Rightarrow$ prolazi test $\Rightarrow$ dobri su izgledi da je broj n prost.