1. 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.

2. U nekoj banci se za šifriranje troznamenkastih PIN-ova koristi RSA kriptosustav s javnim ključem (n, e), gdje je $n = 1411 = 17 \cdot 83$ i $e = 835$. Koji PIN ima Alice ako je šifrat njezinog PIN-a 002?

3. 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

$$\begin{aligned} n_1 &= 217, \qquad c_1 = 153, \\ n_2 &= 299, \qquad c_2 = 226, \\ n_3 &= 319, \qquad c_3 = 298, \end{aligned}$$

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

4. 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

$$\begin{aligned} n_1 &= 161, \qquad c_1 = 57, \\ n_2 &= 247, \qquad c_2 = 96, \\ n_3 &= 493, \qquad c_3 = 272, \end{aligned}$$

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

5. Zadan je RSA kriptosustav s javnim ključem $(n, e) = (69627997, 43206989)$. Odredite pomoću Wienerovog napada skup mogućih tajnih ključeva d ako je poznato da vrijedi $d < \frac{1}{3}\sqrt[4]{n}$.

6. Zadan je RSA kriptosustav s javnim ključem $(n, e) = (60677801, 47474687)$. Odredite pomoću Wienerovog napada skup mogućih tajnih ključeva d ako je poznato da vrijedi $d < \frac{1}{3}\sqrt[4]{n}$.

7. U RSA kriptosustavu je $n = pq = 51809$, gdje su p i q prosti brojevi. Špijuniranjem ste otkrili da je $\sigma(n) = 52416$ ($\sigma(n)$ je suma djelitelja broja n). Odredite p i q bez poznavanja faktorizacije od n.
   Uputa: Iskoristite multiplikativnost od σ i Vièteove formule.

8. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2773, 47, 59),$$

   dešifrirajte šifrat $y = 2729$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

9. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2021, 43, 47),$$

   dešifrirajte šifrat $y = 917$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

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

11. Zadan je ElGamalov kriptosustav s ključem $K = (p = 41, \alpha = 6, a = 10, \beta = 32)$. Dešifrirajte šifrat $(y_1, y_2) = (11, 21)$.

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

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

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

13. Zadan je Merkle-Hellmanov kriptosustav s ključem $K = (v, p, a, t)$ gdje je

$$v = (3, 6, 24, 48, 95, 187, 380, 760),$$
$$p = 1571,\ a = 111,$$
$$t = (333, 666, 1093, 615, 1119, 334, 1334, 1097).$$

    Dešifrirajte šifrat $y = 3379$.