0. (za ogrevanje)

   Naj bo $n = pq$, kjer sta p in q različni lihi praštevili in $ed \equiv 1 (\mathrm{mod}\ \varphi(n))$. RSA enkripcijska funkcija je $E(x) = x^e \bmod n$, RSA dekripcijska funkcija pa je $D(x) = x^d \bmod n$. Najprej se prepričaj, da je $D(E(x)) = x$ za $x \in \mathbb{Z}_n^*$, nato pa pokaži, da ista trditev velja za vsak $x \in \mathbb{Z}_n$.

1. Reši eno izmed nalog 5.15, 5.16, 5.17, 5.19, 5.22 in 5.23. Prve tri naloge ilustrirajo težave protokolov z RSA sistemom. V četrti nalogi morate dokazati, da je verjetnost napake v Solovay-Strassen testu praštevilčnosti kvečjemu 1/2 (dobite štiri napotke). V zadnjih dveh nalogah pa pobližje spoznate nekatere lastnosti Las Vegas probabilističnega algoritma.

2. (a) Naslednje je varianta faktorizacijske metode z naključnimi kvadrati, ki je poznana pod imenom metoda kvadratnega rešeta (angl. quadratic sieve algorithm).
   Naj bo n število, ki ga želimo faktorizirati, $m = \lfloor \sqrt{n} \rfloor$ in $q(x) = (x+m)^2 - n$. Iz

   $$q(x) = (x+m)^2 - n \equiv (x+m)^2 \ (\mathrm{mod}\ n)$$

   sledi, da je polinom $q(x)$ kvadratni ostanek po modulu n za poljubno število x.
   Majhni naključni kvadrati so izbrani s pomočjo $x = \pm 0, \pm 1, \pm 2, \ldots$.
   Na primer naj bo $n = 10057$. Potem je $m = 100$ in $q(x) = (x+100)^2 - 10057$.
   Za $x = 0$ je $q(0) = -57 = -3 \cdot 19$, kar nam da relacijo

   $$100^2 \equiv -3 \cdot 19 \ (\mathrm{mod}\ 10057).$$

   Naprej nadaljujemo kot je opisano v učbeniku (str. 188).
   Uporabi metodo kvadratnega rešeta za faktorizacijo števila $n = 373831$. Za faktorsko bazo vzemi $B = \{1, 2, 3, 5, 7, 11, 13, 17, 19, 23\}$. Ker ima faktorska baza 10 elementov, algoritem pravi, da moraš najti vsaj 11 relacij. V tej nalogi jih poišči le toliko kolikor jih potrebuješ, da po produkt nekaterih izmed njih dal popolna kvadrata na obeh straneh.

   (b) Število 5 je generator grupe $\mathbb{Z}_{1223}^*$. Z metodo veliki korak-mali korak izračunaj $\log_5 525$ v grupi $\mathbb{Z}_{1223}$.

3. Naj bo p liho praštevilo, α in γ pa generatorja grupe $\mathbb{Z}_p^*$. Predpostavimo, da imamo učinkovit algoritem A za računanje diskretnega algoritma za bazo α. Pokaži, da je možno uporabiti ta algoritem za učinkovito računanje diskretnega algoritma za bazo γ.

4. Število $\alpha = 107$ je generator grupe $\mathbb{Z}_{541}$. Privzemimo, da uporabljamo metodo index calculus za računanje diskretnega logaritma $\log_\alpha \beta$, kjer je $\beta = 246$.
   Najprej izberemo faktorsko bazo $B = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$.
   Nato določimo logaritme elementov iz B: $\log_\alpha 2 = 299$, $\log_\alpha 3 = 316$, $\log_\alpha 5 = 344$, $\log_\alpha 7 = 462$, $\log_\alpha 11 = 185$, $\log_\alpha 13 = 347$, $\log_\alpha 17 = 441$, $\log_\alpha 19 = 382$, $\log_\alpha 23 = 52$, $\log_\alpha 29 = 261$.
   Sam dokončaj tretjo fazo (računanje diskretnega logaritma $\log_\alpha \beta$).

5.15 Ta naloga prikazuje *napako protokola*. Opisan je primer, ko nasprotnik lahko dešifrira tajnopis, ne da bi ugotovil ključ, če se kriptosistem uporablja nepazljivo. (Ker nasprotnik ne ugotovi ključa, tega ne imenujemo kriptoanaliza.) Nauk je, da ni dovolj uporabiti "varen" kriptosistem, da zagotovimo "varno" komunikacijo.

Predpostavimo, da Bojan uporablja RSA kriptosistem z velikim modulom n, za katerega ne moremo najti faktorizacije v doglednem času. Predpostavimo, da Anita pošlje Bojanu sporočilo, tako da vsako črko predstavi s številom med 0 in 25 (tj. $A \leftrightarrow 0$, $B \leftrightarrow 1$, itd.) in nato zašifrira vsako črko posebej.

(a) Opiši, kako lahko Oskar z lahkoto dekriptira sporočilo, ki je zašifrirano na ta način.

(b) Ilustriraj napad z dekriptiranjem naslednjega tajnopisa (uporabljen je bil RSA sistem z $n = 18721$ in $b = 25$), ne da bi faktoriziral n:

$$365, 0, 4845, 14930, 2608, 2608, 0.$$

5.16 V tej nalogi je prikazan še en primer napake protokola v zvezi z RSA kriptosistemom (odkril ga je Simmons); imenuje se *napaka skupnega modula*. Predpostavimo, da Bojan uporablja RSA kriptosistem z modulom n in šifrirnim eksponentom b_1, Cene pa uporablja RSA kriptosistem z (istim) modulom n in šifrirnim eksponentom b_2. Nadalje predpostavimo, da je $D(b_1, b_2) = 1$. Oglejmo si situacijo, ki nastane, če Anita zašifrira isti čistopis x za Bojana in za Ceneta. Torej izračuna $y_1 = x^{b_1} \bmod n$ in $y_2 = x^{b_2} \bmod n$ ter nato pošlje y_1 Bojanu in y_2 Cenetu. Predpostavimo, da Oskar prestreže y_1 in y_2 in opravi izračune, nakazane na Sliki 1.

Vhodni podatki: n, b_1, b_2, y_1, y_2
1. izračunaj $c_1 = b_1^{-1} \bmod b_2$
2. izračunaj $c_2 = (c_1 b_1 - 1)/b_2$
3. izračunaj $x_1 = y_1^{c_1}(y_2^{c_2})^{-1} \bmod n$

Slika 1: Napaka skupnega modula pri RSA kriptosistemu

(a) Dokaži, da je vrednost x_1, izračunana v tretjem koraku na Sliki 1, dejansko čistopis x. Torej lahko Oskar dekriptira sporočilo, ki ga je poslala Anita, čeprav je kriptosistem "varen".

(b) Prikaži napad za primer $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$ in $y_2 = 14702$.

5.17 Še ena napaka protokola v zvezi z RSA kriptosistemom. Recimo, da trije uporabniki omrežja, npr. Bojan, Branko in Boris, uporabljajo isti javni šifrirni eksponent $b = 3$. Označimo njihove module z n_1, n_2 in n_3. Predpostavimo, da Anita zašifrira in pošlje isti čistopis Bojanu, Branku in Borisu, tj. izračuna $y_i = x^3 \bmod n_i$, $1 \leq i \leq 3$. Opiši, kako lahko Oskar iz danih y_1, y_2 in y_3 izračuna x, ne da bi faktoriziral katerikoli modul.

5.19 Predpostavimo, da je A deterministični algoritem, ki za dane vhodne podatke: RSA modul n, šifrirni eksponent b in tajnopis y bodisi dekriptira y bodisi ne vrne odgovora. Pokaži, kako lahko uporabiš A kot orakelj v Las Vegas dekriptirnem algoritmu z verjetnostjo uspeha ε ob predpostavki, da A lahko dekriptira $\varepsilon(n-1)$ tajnopisov.

5.22 V tej nalogi dokažeš, da je verjetnost napake v Solovay-Strassenovem testu praštevilčnosti kvečjemu 1/2. Označimo z $\mathbb{Z}_n^*$ grupo obrnljivih elementov po modulu n. Definirajmo

$$G(n) = \left\{ a : a \in \mathbb{Z}_n^*, \left(\tfrac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n} \right\}.$$

(a) Dokaži, da je $G(n)$ podgrupa grupe $\mathbb{Z}_n^*$. Torej po Lagrangevem izreku sledi (če $G(n) \neq \mathbb{Z}_n^*$)

$$|G(n)| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{n-1}{2}.$$

(b) Predpostavimo, da je $n = p^k q$, kjer sta p in q lihi števili, p praštevilo, $k \geqslant 2$ in $D(p,q) = 1$. Naj bo $a = 1 + p^{k-1}q$. Dokaži, da

$$\left(\tfrac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}.$$

NASVET Uporabi binomsko formulo za izračun $a^{(n-1)/2}$.

(c) Predpostavimo, da je $n = p_1 \cdots p_s$, kjer so p_i različna liha praštevila. Denimo, da je $a \equiv u \pmod{p_1}$ in $a \equiv 1 \pmod{p_2 p_3 \cdots p_s}$, kjer u ni kvadratični ostanek po modulu p_1 (tak a obstaja po kitajskem izreku o ostankih). Dokaži, da velja

$$\left(\tfrac{a}{n}\right) \equiv -1 \pmod{n},$$

toda

$$a^{(n-1)/2} \equiv 1 \pmod{p_2 p_3 \cdots p_s}$$

in zato

$$a^{(n-1)/2} \not\equiv -1 \pmod{n}.$$

(d) Dokaži: če je n lih in sestavljen, je $|G(n)| \leq (n-1)/2$.

(e) Iz zgornjih točk zaključi, da je verjetnost napake Solovay-Strassenovega testa praštevilčnosti kvečjemu 1/2.

5.23 Predpostavimo, da imamo Las Vegas algoritem z verjetnostjo neuspeha enako ε.

(a) Dokaži, da je verjetnost, da prvič uspemo na n-tem koraku, enaka $p_n = \varepsilon^{n-1}(1-\varepsilon)$.

(b) Povprečno (pričakovano) število poizkusov, da dosežemo uspeh, je

$$\sum_{n=1}^{\infty} n \cdot p_n.$$

Pokaži, da je to povprečje enako $1/(1-\varepsilon)$.

(c) Naj bo δ pozitivno realno število, manjše od 1. Pokaži, da je potrebno število ponovitev algoritma, da zmanjšamo verjetnost napake pod δ, enako

$$\left\lceil \frac{\log_2 \delta}{\log_2 \varepsilon} \right\rceil.$$