Kriptografija – 5. domača naloga (do petka 27. februarja 2004)

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 4.7, 4.8, 4.9, 4.14, 4.11 in 4.15. 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

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

   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

   $$100^2 \equiv -3 \cdot 19 \pmod{10057}.$$

   Naprej nadaljujemo kot je opisano v knjigi (str. 153).
   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 in $\prod_{i=1}^{r} q_i^{c_i}$ praštevilska faktorizacija števila $p-1$.

   (a) Dokaži, da je $\alpha \in \mathbb{Z}_p^*$ generator grupe $\mathbb{Z}_p^*$ natanko tedaj, ko je

   $$\alpha^{(p-1)/q_i} \not\equiv 1 \pmod{p} \quad \text{za } i = 1, \ldots, r.$$

   (b) Naj bo α generator grupe $\mathbb{Z}_p^*$. Dokaži, da je α^t tudi generator grupe $\mathbb{Z}_p^*$ natanko tedaj, ko je $D(t, p-1) = 1$. (Od tod sledi, da ima $\mathbb{Z}_p^*$ natanko $\varphi(p-1)$ generatorjev.)

   (c) Sestavi algoritem, ki za podatke: praštevilo p in praštevilsko faktorizacijo števila $p-1$, poišče generator grupe $\mathbb{Z}_p^*$ in oceni časovno zahtevnost svojega algoritma.
   (Lahko uporabiš naslednjo neenakost: $\varphi(n) > n/(\ln \ln n)$ za vsak $n \geq 5$.

4. 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.

5. 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 $\log_\alpha \beta$).