Kriptografija in teorija kodiranja – 2. domača naloga

(do srede, 31. marca 2010 – oddaja v asistentov predalček na Jadranski 21)

Naloge rešujte samostojno. Odgovori in rešitve naj bodo jasne, pregledne in dobro utemeljene!

1. Anita in Bojan sta se dogovorila, da izbereta en dober par praštevil p in q in uporabljata skupni modul $n = pq$. Predpostavimo, da Anita in Bojan izbereta zaporedoma tuji si enkripcijski potenci e_a in e_b. Dokaži, da lahko napadalec učinkovito odšifrira sporočili, ki sta poslani obema khrati. (Z drugimi besedami: za dana števila n, e_a, e_b, $c_a = m^{e_a} \pmod n$, $c_b = m^{e_b} \pmod n$ pokaži, da lahko napadalec učinkovito izračuna m.)

2. 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 $n \geq 5$.

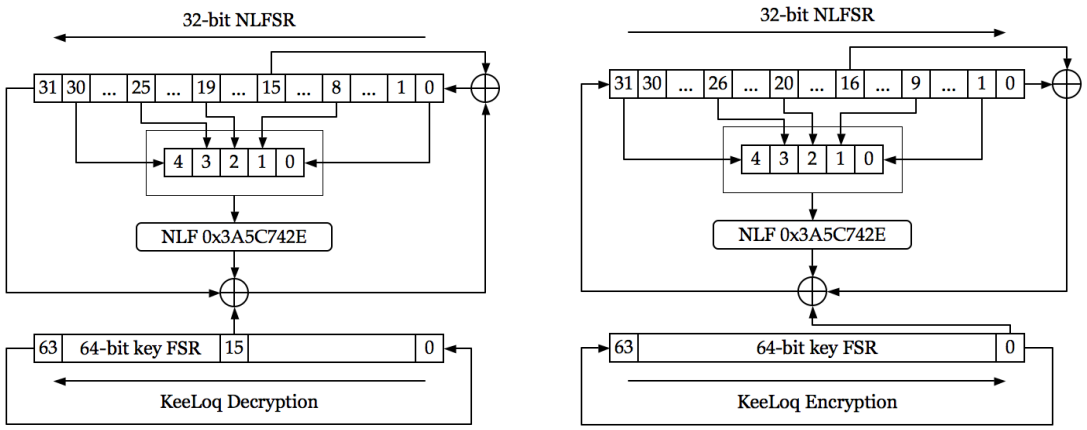
4. Naj bo p liho praštevilo, α in γ pa generatorja grupe $\mathbb{Z}^*_p$. Predpostavimo, da imamo učinkovit algoritem A za računanje diskretnega algoritma za bazo α. Pokaži, da je možno uporabiti ta algoritem za učinkovito računanje diskretnega algoritma za bazo γ.

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 $\log_\alpha \beta$).

6. Bločna šifra **KeeLoq** uporablja 64-bitne ključe in šifrira 32-bitne bloke z izvajanjem svojega enobitnega NLFSR v 528 krogih. Opišimo en njen krog. NLFSR povratna funkcija je `0x3A5C742E` oziroma

$$F(a,b,c,d,e) = d \oplus e \oplus ac \oplus ae \oplus bc \oplus be \oplus cd \oplus de \oplus ade \oplus ace \oplus abd \oplus abc.$$

Pri šifriranju uporabi bite 1, 9, 20, 26 in 31 stanja NLFSR za vhod, pri odšifriranju pa bite 0, 8, 19, 25 in 30. Nato pa uporabimo njen izhod za XOR z dvema bitomo iz stanja NLFSR (0 in 16 pri šifriranju ter 31 in 15 pri odšifriranju) in enim bitom ključa (bit 0 iz stanja ključa pri šifriranju in bit 15 pri odšifriranju), da ga uporabimo za povratni bit (fed back) v NLFSR stanje. Glej sliko, ki opiše tudi smer zanika tako pri stanju ključa kakor tudi stanja NLFSR. Uporaba te šifre se uporablja pri večini daljincev, npr. pri podjetjih kot so Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, Volkswagen Group, Clifford, Shurlok, Jaguar itd. Glej npr. `http://en.wikipedia.org/wiki/KeeLoq`.



Dokaži, da je odšifriranje res inverzna operacija od šifriranja.

7. Naj bo $\mathbb{F}$ poljuben končen obseg. Dokaži, da je trinom $x^n + x^k + 1$ nerazcepen v $\mathbb{F}$ natanko tedaj, ko je v $\mathbb{F}$ nerazcepen trinom $x^n + x^{n-k} + 1$.