

## Kriptografija in teorija kodiranja – 5. domača naloga

(do ponedeljka 25. maja 2009)

---

1. Naj bo  $\alpha$  generator multiplikativne grupe  $\mathbb{Z}_p^*$  in naj bo  $H$  zgoščevalna funkcija;  $p$ ,  $\alpha$  in  $H$  so javno dostopni. Naj bosta  $a$  in  $\alpha^a \bmod p$  zaporedoma zasebni in javni ključ osebe  $A$ . Ponovimo, da za podpis sporočila  $M \in \{0,1\}^*$  z ElGamalovo shemo, oseba  $A$  izbere naključno število  $k$ ,  $1 \leq k \leq p-2$ , tako da je  $D(k, p-1) = 1$  in izračuna  $r = \alpha^k \bmod p$ ,  $m = H(M)$  ter  $s = k^{-1}(m - ar) \bmod (p-1)$ . Podpis osebe  $A$  je par  $(r, s)$ .

Predpostavimo, da oseba  $B$ , ki preverja podpis osebe  $A$ , ne preveri, če število  $r$  leži na intervalu  $[0, p-1]$ . Ponaredi podpis, ki ga bo oseba  $B$  sprejela za podpis osebe  $A$ ?

2. Naj bo  $\alpha = 13$  generator multiplikativne grupe  $\mathbb{Z}_p^*$ , kjer je  $p = 13q + 1$ ,  $q \in \mathbb{N}$ , tako veliko praštevilo, da je problem diskretnega logaritma računsko nedosegljiv. Predpostavimo, da je Anita podpisala sporočilo  $m$  z ElGamalovim podpisom in pri tem uporabila svoj zasebni ključ  $a$  in svoj javni ključ  $y_A = \alpha^a \bmod p$ . Naj bo  $t = (p-3)/2$ ,  $r = q = (p-1)/13$  in  $s = t(H(m) - rz) \bmod (p-1)$ , kjer je  $13^{rz} \equiv y_A^q \pmod{p}$ .

(a) Pokaži, da lahko napadalec hitro najde tako število  $z$ , da je  $13^{rz} \equiv y_A^q \pmod{p}$ .

(b) Pokaži, da je  $q \equiv -13^{-1} \pmod{p}$  in od tod  $q^t \equiv 13 \pmod{p}$ , če je  $p \equiv 1 \pmod{4}$ .  
Namig  $\alpha^{(p-1)/2} = 1$ .

(c) Če je  $p \equiv 1 \pmod{4}$ , pokaži, da je  $(r, s)$  res podpis sporočila  $m$ .

(d) Če je  $p \equiv 3 \pmod{4}$  in je število  $H(m) - rz$  sodo, pokaži, da je  $(r, s)$  res podpis sporočila  $m$ .

3. Naj bo  $p$  praštevilo,  $q$  praštevilo, ki deli  $p-1$ , in naj ima element  $\alpha \in \mathbb{Z}_p^*$  red  $q$ . Oseba  $A$  si izbere za svoj zasebni ključ par  $(a, u)$  in  $(b, B)$ , kjer je

$$b = \alpha^{u^{-1}} \bmod p \quad \text{in} \quad B = ua \bmod q,$$

za svoj javni ključ. Število  $m$  naj bo sporočilo, ki ga bo oseba  $A$  podpisala.

Oseba  $A$  izračuna svoj podpis  $(r, s)$  na naslednji način:

(a) izberi naključno število  $k$ ,  $1 \leq k \leq q-1$ , in izračunaj  $r = \alpha^k \bmod p$ ,

(b) izračunaj  $e = H(m||r)$ , kjer je  $H$  zgoščevalna funkcija,

(c) izračunaj  $s = u(k + ae) \bmod q$ .

Preverjanje podpisa  $(r, s)$  z javnim ključem  $(b, B)$  in javnimi parametri  $p, q$ , ki deli  $p-1$ , in  $\alpha \in \mathbb{Z}_p^*$  reda  $q$ :

(a) izračunaj  $v = s - Be \bmod q$ ,

(b) izračunaj  $r' = b^v \bmod p$ ,

(c) izračunaj  $e' = H(m||r')$ ,

(d) sprejmi podpis če in samo če je  $e = e'$ .

Pokaži, da preverjanje podpisa deluje. Ali je ta shema za digitalni podpis varna?