

# KRYPTOGRAFIA 801698S

Loppukoe 28.01.2008

EI LASKIMIA, EI KÄNNYKÖITÄ

- a) Tiedetään, että  $\mathbb{Z}_{71}^* = \langle 7 \rangle$ . Määrää sellainen luku  $1 \leq a \leq 70$ , että aliryhmän  $D = \langle 7^a \rangle$  kertaluku  $\#D = 10$ .  
b) Määrää lukujen  $a = 700, \sqrt{-1}, 16$  diskreetit logaritmit  $\log_2 a$  ja kertaluvut  $\text{ord } a$  sykklisessä ryhmässä  $\langle 2 \rangle = \mathbb{Z}_{701}^*$ .

- $A$  ja  $B$  käyttävät ElGamal allekirjoitus/kryptaus-järjestelmää ryhmässä  $\mathbb{Z}_{71}^* = \langle 7 \rangle$  ja heidän julkiset avaimet ovat  $k_A = 59, k_B = 6$ . Olkoon  $A$ :n salaiset avaimet (eksponentit)  $a = a' = 3$ , lähetettävä viesti  $m = 42$  sekä

$$\rho : \mathbb{Z}_{71}^* \rightarrow \mathbb{Z}_{70}, \quad \rho(x) = x$$

allekirjoitusyhtälössä käytettävä funktio. Muodosta  $A$ :n lähetämä allekirjoitettu ja kryptattu viesti  $(r, s, k_A, v_A)$ .

- Olkoon  $E = E(\mathbb{Z}_5)$  elliptinen käyrä

$$E : y^2 = x^3 + x - 1 \in \mathbb{Z}_5[x].$$

Tiedetään, että  $\#E(\mathbb{Z}_5) = 9$  sekä  $2Q = (2, 2), 4Q = (0, 2)$ , missä  $Q = (1, 1) \in E(\mathbb{Z}_5)$ . Määrää ryhmässä  $E(\mathbb{Z}_5)$  monikerrat  $nQ, n = 0, 1, 2, \dots, 8$  sekä  $\text{ord}(3, 3)$ .

- $A$  ja  $B$  käyttävät 3. tehtävän ryhmää  $H = \langle Q \rangle$ . Olkoot  $A$ :n ja  $B$ :n julkiset avaimet  $K_A = (2, 2)$  ja  $K_B = (3, 2)$ .

a) Määrää  $A$ :n ja  $B$ :n yhteinen Diffie-Hellman avain  $K_{A,B} = (c_1, c_2)$ .

b)  $A$  kryptaa viestin  $M = (u_1, u_2) \in \mathbb{Z}_5^2$  Menezes-Vanstone kryptosanomaksi  $(y_1, y_2)$  ja lähettää  $B$ :lle sanoman  $(K_A, y_1, y_2) = ((2, 2), 3, 2)$ . Määrää viesti  $M$ .

- Olkoot  $n \in \mathbb{Z}^+$  ja  $q \in \mathbb{P}$  sellaisia, että  $q|n-1$  ja  $q > \sqrt{n}-1$ . Oletetaan vielä, että on olemassa sellainen  $a \in \mathbb{Z}$ , että

$$a^{n-1} \equiv 1 \pmod{n}, \quad \text{syt}(a^{(n-1)/q} - 1, n) = 1.$$

Todista tällöin, että  $n \in \mathbb{P}$ .