KRYPTOGRAFIA 801698S

Loppukoe 21.4.2008

EI LASKIMIA, EI KÄNNYKÖITÄ

1. 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 $\operatorname{ord} a$ syklisessä ryhmässä $\langle 2 \rangle = \mathbb{Z}_{701}^*$.

2. A ja B käyttävät El-Gamal kryptausjärjestelmää ryhmässä $\mathbb{Z}_{71}^* = \langle 7 \rangle$. $k_A = 9, k_B = 59$. A lähettää B:lle lukuparin $(k_A, v_A) = (9, 2)$, josta B purkaa viestin m_1 käyttäen salaista eksponenttia $b = 3$.

   a) $m_1 =?$

   b) Oletetaan, että $C \neq A, B$ tuntee viestin m_1. Nyt C näkee uuden lukuparin $(k_A, v'_A) = (9, 20)$, josta C määrää uuden viestin $m_2 =?$

3. 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, $n = 0, 1, 2, ..., 8$ sekä $\operatorname{ord}(3, 3)$.

4. 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.

5. Johda elliptisen käyrän

   $$E : y^2 = x^3 + ax + b \; ; \; \triangle \neq 0$$

   yhteenlaskukaavat lähtien Jacobin periaatteesta: Projektiivisen tason kolmannen asteen käyrän pisteet $P \neq Q$ ja niiden kautta kulkevan suoran ja käyrän kolmas leikkauspiste R toteuttavat relaation

   $$P + Q + R = \mathcal{O},$$

   missä $\mathcal{O} = [0, 1, 0]$.