KRYPTOGRAFIA 801698S

Loppukoe 8.3.2010

EI LASKIMIA, EI KÄNNYKÖITÄ

1. a) Määrittele pseudoalkulukujen joukko PSP_b ja Eulerin pseudodalkulukujen joukko ESP_b kannan b suhteen sekä Carmichaelin luvut.

   b) Osoita, että $ESP_b \subseteq PSP_b$.

2. 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

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

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

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 $\mathrm{ord}(3, 3)$.

4. Olkoot $q \equiv 1 \pmod 5$ ja $\langle \beta \rangle = \mathbb{F}_q^*$. Asetetaan $z = (q-1)/5$ ja $\tau_j = \beta^{zj}$, kun $j = 0, 1, 2, 3, 4$. Tiedetään, että käyttäjän A_i Diffie-Hellman salainen avain on muotoa

   $$a_i = 31021980 + i, \ i \in \{1, 3, 7, 9\}.$$

   Kenen käyttäjän $X \in \{A_1, A_3, A_7, A_9\}$ julkinen avain on k_X, jolle pätee $k_X^z = \tau_2$?

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 $\mathcal{O} = [0, 1, 0]$.