KRYPTOGRAFIA 801698S (5op)

Loppukoe 26.9.2011 EI LASKIMIA, OPISKELIJANUMERO

1. a) Näytä, että $\sinh x = \mathcal{O}(e^x)$.

b) Määrää diskreetit logaritmit

$$\log_{\overline{2}} \alpha, \quad \alpha = -\overline{1}, \overline{7} \in \mathbb{Z}_{25}^*.$$

2. 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 $k_X^z = \tau_2$?

Tehtävissä 3., 4. ja 5. käytetään elliptistä käyrää

$$\overline{E} = \overline{E}(\mathbb{Z}_5) = \{[x, y, z] \in \mathbb{P}^2(\mathbb{Z}_5) \mid y^2 z = x^3 + xz^2 - z^3\}, \tag{1}$$

jolla on 9 pistettä.

3. Määrää käyrällä $\overline{E}$ olevat

a) affiinit pisteet.

b) ääretönpisteet.

4. Olkoon $P = (0, 3)$. Tiedetään, että $3P = (3, 3)$ ja $4P = (2, 2)$ ryhmässä $\overline{E}$.

a) Määrää $-(2, 2)$.

b) Määrää monikerrat nP, kun $n = 0, 1, ..., 8, 9$.

c) diskreetti logaritmi $\log_P(2, 3)$.

5. Seuraavassa A ja B käyttävät ElGamal/Menezes-Vanstone kryptaus-järjestelmiä ryhmässä $H = \langle (0, 3) \rangle$. Olkoot A:n ja B:n julkiset avaimet $K_A = (1, 1)$ ja $K_B = (3, 3)$.

a) Mikä on yhteinen avain $K_{A,B}$?

b) Mikä on viestin $(2, 2)$ ElGamal kryptoviesti V_A?

c) Mikä on A:n B:lle lähettämään Menezes-Vanstone kryptoviestiin $(y_1, y_2) = (3, 0)$ piilotettu viesti (u_1, u_2)?.