KRYPTOGRAFIA (Uusi kurssi 5op)

Loppukoe 17.5.2010 EI LASKIMIA, OPISKELIJANUMERO

1. a) Osoita, että $\mathbb{Z}_{25}^* = \langle \overline{2} \rangle$.
b) Määrää diskreetit logaritmit

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

Tehtävissä 2. ja 3. käyttäjät A ja B käyttävät ElGamal allekirjoitus/kryptaus-järjestelmää ryhmässä $\mathbb{Z}_{25}^* = \langle 2 \rangle$. Olkoot A:n salaiset avaimet (eksponentit) $a = 3$ ja $a' = 7$, sekä B:n salaiset avaimet $b = 9$ ja $b' = 3$. Olkoon A:n lähettämä viesti $m = 11$ sekä olkoon

$$\rho : \mathbb{Z}_{25}^* \to \mathbb{Z}_{20}, \quad \rho(x) = x \pmod{20}$$

allekirjoitusyhtälössä käytettävä funktio.

2. a) Muodosta yhteinen avain $k_{A,B}$.
b) Muodosta A:n lähettämä kryptattu viesti v_A.

3. a) Muodosta A:n lähettämä allekirjoitettu ja kryptattu viesti (r, s, k_A, v_A).
b) Suorita käyttäjän B tekemä viestin dekryptaus ja varmennus.

Tehtävissä 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.

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) Selvitä 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)?