KRYPTOGRAFIA (Uusi kurssi 5op)

2. Välikoe 10.5.2010 EI LASKIMIA, OPISKELIJANUMERO
(Vähintään 14 pistettä.)

1. Olkoon

$$g(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x], \quad \mathbb{Z}_3[x]/(g(x)) = \mathbb{F}_{27}, \quad g(\alpha) = 0.$$

a) Osoita laskemalla, että

$$\alpha^4 = \alpha^2 + 2\alpha, \quad \alpha^8 = 2\alpha^2 + 2, \quad \alpha^{13} = -1. \qquad \text{(5 pistettä)}$$

b) Miksi a) kohdan nojalla α on kunnan $\mathbb{F}_{27}$ primitiivialkio eli $\langle\alpha\rangle = \mathbb{F}_{27}^*$? (3p)

c) Määrää

$$\log_\alpha(-1), \quad \log_\alpha\left(\frac{\alpha^2 + 2\alpha}{2\alpha^2 + 2}\right). \qquad (2p)$$

Tehtävissä 2., 3. ja 4. käytetään elliptistä käyrää

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

jolla on 9 pistettä.

2. Määrää käyrällä $\overline{E}$ olevat
a) affiinit pisteet.
b) ääretönpisteet.

3. Olkoon $P = (0, 3)$. Tiedetään, että $3P = (3, 3)$ ja $4P = (2, 2)$ ryhmässä $\overline{E}$.
a) Määrää $-(2, 2)$. (2p)
b) Määrää monikerrat nP, kun $n = 0, 1, ..., 8, 9$. (8p)

4. 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 $K_{A,B}$? (3p)

b) Mikä on viestin $(2, 2)$ ElGamal kryptoviesti V_A? (3p)

c) Mikä on A:n B:lle lähettämään Menezes-Vanstone kryptoviestiin $(y_1, y_2) = (3, 0)$ piilotettu viesti (u_1, u_2)? (4p).