KRYPTOGRAFIA (Uusi kurssi 5op)

1. Välikoe 19.4.2010 EI LASKIMIA, EI PUHELIMIA

1. Näytä, että

a) $\sinh x = \mathcal{O}(e^x)$.

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

c) 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 $\mathbb{Z}_{71}^* = \langle 7 \rangle$. Olkoot A:n salaiset avaimet (eksponentit) $a = 3$ ja $a' = 9$, sekä B:n salaiset avaimet $b = 17$ ja $b' = 11$. Olkoon A:n lähettämä viesti $m = 41$ sekä olkoon

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

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.

4. Olkoon ryhmän H kertaluku h ja $a \in H$. Osoita, että potenssin a^r, $1 \leq r \leq h-1$, laskemiseen tarvitaan korkeintaan $\mathcal{O}(h)$ ryhmän H laskutoimitusta.