MAT-63256 Mathematical Cryptology Tentti 2.10.2014

Tentaattori: FOLDES / RUOTTINEN

Huom! Mukana ei saa olla kirjallisuutta, tietokoneita eikä taulukoita. Funktiolaskin on sallittu.

1. Selosta lyhyesti klassisia kryptosysteemejä AFFINE ja HILL, niiden toimintaa ja murtomahdollisuuksia.

2. **a)** Etsi jokin $\mathbb{Z}_2[x]$:n toisen asteen jaoton polynomi $p(x)$.
   b) Konstruoi äärellinen kunta $\mathbb{F}_{2^2}$ jäännösluokkina modulo $p(x)$. Esitä kunnan yhteen- ja kertolaskutaulut.
   c) Miksei tulos ole $\mathbb{Z}_4$?

3. Selosta kryptosysteemiä RSA, sen toimintaa ja mihin sen turvallisuus perustuu.

4. Diffie–Hellman-avainjakosysteemissä (ryhmässä $\mathbb{Z}_p^*$) on käytössä suuri alkuluku p ja primitiivinen juuri g modulo p. Osapuoli i on huolimaton ja näin vihamielinen taho A saa tietoonsa hänen salaisen avaimensa x_i sekä julkisen avaimensa $X_i = (g^{x_i}, \mathrm{mod}\ p)$ ja lisäksi alkuluvun p, mutta ei generaattoria g. Salainen avain x_i valittiin siten, että myös X_i on primitiivinen juuri modulo p (mikä on edullista). Jos A epäilee näin olevan, hän saa helposti lasketuksi myös g:n. Selosta miten?

5. Kuinka suurten kvanttitietokoneiden tulo muuttaisi nykyistä tilannetta kryptauksessa?

In English ⟶⟶⟶