MAT-52600 Matemaattinen kryptologia Tentti 23.5.2008

Huom! Mukana ei saa olla kirjallisuutta, tietokoneita eikä taulukoita. Laskuvälineet ovat sallittuja.

1. Selosta lyhyesti klassisia kryptosysteemejä **a)** AFFINE, **b)** HILL ja **c)** VIGENÈRE, niiden toimintaa ja murtomahdollisuuksia.

2. AES-kryptosysteemi, sen käyttö ja rakenne pääpiirteissään.

3. Algoritmi A *murtaa* julkisen avaimen kryptosysteemin *osittain*, jos

- saatuaan syötteenä julkisen avaimen k_1 sekä sitä käyttäen kryptatun kryptotekstin $c = e_{k_1}(w)$ algoritmi A joko dekryptaa c:n ja tulostaa vastaavan selvätekstin w tai sitten ilmoittaa luopuvansa,
- kullekin julkiselle avaimelle k_1 algoritmi A dekryptaa ainakin $100\,\theta$ % kaikista k_1:tä käyttäen kryptatuista kryptoteksteistä (tässä θ on tunnettu positiivinen luku, joka ei riipu julkisesta avaimesta), ja
- A on deterministinen ja polynomiaikainen.

Totea, että jos algoritmi A murtaa osittain RSA-kryptosysteemin, niin A voidaan muuntaa polynomiaikaiseksi Las Vegas -tyyppiseksi stokastiseksi algoritmiksi, jolla voidaan murtaa ko. systeemi, ts. dekryptata mielivaltainen annettu kryptattu viesti. (Kuten tavallista, jos RSAn julkinen avain on $k_1 = (n, a)$, niin rajoitutaan selväteksteihin w, joille $\mathrm{syt}(w, n) = 1$.)

(Näin ollen RSAlle ei näillä tiedoin ole sen osittain murtavaakaan algoritmia. Vastaava tulos pätee myös ELGAMALille.)

4. **a)** Muodosta multiplikatiivinen ryhmä $\mathbb{Z}_7^*$ eli anna sen ryhmätaulu, jossa on kaikkien ryhmäoperaatioiden tulokset, ja käänteisalkiot.

b) Ryhmä $\mathbb{Z}_7^*$ on syklinen. Etsi sen kaikki generaattorit (primitiiviset juuret modulo 7). Muodosta vielä kullekin generaattorille g sitä vastaava indeksitaulu eli laske g-kantaiset diskreetit logaritmit.

5. Mitä on avainjako kvanttimenetelmällä ja miten se poikkeaa esimerkiksi Diffie–Hellman-menetelmästä?

In English ⟶⟶⟶