

# MAT-52600 Matemaattinen kryptologia Tentti 15.5.2006

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

1. AES-kryptosysteemi, mihin sitä käytetään ja millainen on sen rakenne pääpiirteissään.
2.
  - a) Etsi kaikki primitiiviset juuret modulo 11.
  - b) Valitse yksi näistä primitiivisistä juurista, merkitään  $g$ , ja etsi diskreetit logaritmit  $\log_g \bar{x}$  kaikille jäännösluokille  $\bar{x} \neq \bar{0}$  modulo 11.
3. Aviopari A ja B pystytti RSA-kryptaukseen perustuvan systeemin, jolla voi lähettää heille salattuja viestejä. Tämä tapahtui seuraavasti. Ulkopuolinen luotettu osapuoli T valitsi salassa suuret jotakuinkin yhtä pitkät alkuluvut  $p$  ja  $q$ , kertoi ne yhteen luvuksi  $n = pq$  sekä valitsi kummallekin puolisolalle satunnaisen salaisen dekryptauseksponentin ja laskeki vastaavat kryptauseksponentit. Puolisolle A hän toimitti luvun  $n$ , sekä salaisen dekryptauseksponentin  $b_A$  ja kryptauseksponentin  $a_A$ . Vastaavasti T toimitti puolisolalle B luvut  $n$ ,  $b_B$  ja  $a_B$ . Luvut  $n$ ,  $a_A$  ja  $a_B$  julkaistiin käyttöohjeineen. Tällöin kävi ilmi, että  $\text{syt}(a_A, a_B) = 1$ .
  - a) Pystyykö A avaamaan käsiinsä saamiaan B:lle lähetettyjä kryptattuja viestejä? Perustele vastauksesi!
  - b) Ulkopuolinen taho pystyy avaamaan viestin, jonka se saa käsiinsä molemmille puolisoille kryptattuna lähetettynä. Miten?
4. ELGAMAL-kryptosysteemi, miten se toimii, mihin sitä käytetään ja miten se pystytetään.
5. Tiivistefunktiot, niiden ominaisuudet ja hyökkäykset niitä vastaan.