T-79.5501 Kryptologia
Tentti
14.12.2005

1. (6 pist) Tarkastellaan salausmenetelmää ja siihen liittyviä satunnaismuuttujia: selväkieli $\mathbf{P}$, salakieli $\mathbf{C}$ ja avain $\mathbf{K}$. Oletetaan, kuten tavallista, että $\mathbf{P}$ ja $\mathbf{K}$ ovat riippumattomat. Todista, että silloin $\mathrm{H}(\mathbf{P}) \leq \mathrm{H}(\mathbf{C})$, ja että yhtäsuuruus $\mathrm{H}(\mathbf{P}) = \mathrm{H}(\mathbf{C})$ pätee jos ja vain jos $\mathbf{C}$ ja $\mathbf{K}$ ovat riippumattomat.

2. (6 pist) Etsi kokonaisluvut x ja y siten että $14x + 2005y = 12$.

3. Tarkastellaan kahta binaarista lineaarista siirtorekisteriä, joiden kytkentäpolynomit ovat $f(x) = x^4 + x^3 + x^2 + 1$ ja $g(x) = x^3 + x^2 + 1$, missä $g(x)$ on jaoton.

   (a) (3 pist) Laske $\mathrm{lcm}(f(x), g(x))$.

   (b) (3 pist) Olkoon S_1 mielivaltainen, siirtorekisterillä jonka kytkentpolynomi on $f(x)$, generoitu jono. Samoin olkoon S_2 mielivaltainen, siirtorekisterillä jonka kytkentäpolynomi on $g(x)$, generoitu jono. Määritä summajonon $S_1 + S_2$ suurin mahdollinen jakso.

4. (a) (3 pist) Laske Jacobi symbolin

   $$\left(\frac{1223}{2005}\right)$$

   arvo, jakamatta mitään lukuja muilla tekijöillä kuin mahdollisesti luvun 2 potensseilla.

   (b) (3 pist) Osoita, että $2005 = 5 \cdot 401$ on Eulerin pseudo-alkuluku kantaluvun 1223 suhteen.

5. Bob käyttää *Rabinin Salausmenetelmää*. Bobin moduuli on $40741 = 131 \cdot 311$. Alice tietää Bobin moduulin (mutta ei sen tekijöitä). Alice haluaa muistuttaa Bobia eräästä tärkeästä päivämäärästä ja lähettää sen salattuna Bobille. Salakieliteksti on 38176.

   (a) (3 pist) Näytä miten Bob tulkitsee salakielen. Ers tulkinnoista on päivämäärä, jonka Bob hyväksyy ja hylkää muut tulkinnat.

   (b) (3 pist) Alice sattuu näkemään yhden Bobin hylkäämistä tulkinnoista. Se on 20669. Näytä kuinka Alice pystyy nyt jakamaan Bobin moduulin tekijöihin.