T-79.5501 Kryptologia
Tentti
15.5.2007

1. (6 pts) Bluetooth Pairing menettelyssä käytetään PIN-koodia joka koostuu neljästä satunnaisesti valitusta alfanumeerisesta merkistä (36 eri merkkiä). PIN-koodi syötetään laitteen näppäimistöltä, jolloin jokainen merkki koodataan kahdeksan bitin jonoksi. Laske näin muodostetun 32-bittisen PIN-koodin entropia.

2. (6 pts) Boolen funktion g, jolla on n muuttujaa, *lineaarinen struktuuri* määritellään sellaisena bitti-vektorina w, jonka pituus on n ja jolle pätee että $g(x \oplus w) \oplus g(x)$ on vakio. Tarkastellaan Geffen funktiota $g(x) = g(x_1, x_2, x_3) = x_0x_1 \oplus x_0x_2 \oplus x_2$. Osoita että sillä on täsmälleen yksi lineaarinen struktuuri.

3. (6 pts)

   (a) Laske Jacobi symboli

   $$\left(\frac{784}{2041}\right)$$

   suorittamatta muuta tekijöihinjakoa kuin luvun 2 potensseilla jakamista.

   (b) Osoita että 2041 on Eulerin pseudo-alkuluku kannan 784 suhteen. Aputulos: $784^{12} \equiv 1 \pmod{2041}$.

4. Bob käyttää *Rabin Cryptosystem* salausmenetelmää. Bobin moduuli on $40741 = 131 \cdot 311$. Alice tietää Bobin moduulin mutta ei sen tekijöitä. Alice haluaa muistuttaa Bobia tärkeästä päivästä ja lähettää sen salattuna Bobille. Salakieliteksti on 24270.

   (a) (3 pts) Esitä kuinka Bob tulkitsee salakielen. Yksi mahdollisista selväkielistä on tuo tärkeä päivämäärä, jonka Bob tallettaa ja heittää pois muut tulokset.

   (b) (3 pts) Alice sattuu näkemään yhden Bobin pois heittämän tuloksen. Se on 5959. Esitä kuinka Alice pystyy nyt jakamaan Bobin moduulin tekijöihin.

5. (6 pts) Luvun $\alpha = 14$ kertaluku multiplikatiivisessa ryhmässä $\mathbb{Z}^*_{157}$ on 13. On annettu että luku $\beta = 93$ on luvun α generoimassa aliryhmässä. Käyttäen Shanksin algoritmia laske luvun $\beta = 93$ diskreetti logaritmi kannan $\alpha = 14$ suhteen, eli ratkaise yhtälö

   $$14^x \equiv 93 \pmod{157}.$$