T-110.503 Kryptologian perusteet
Loppukoe
08.01.2003

1. (6 pist.) Tarkastellaan binaarista lineaarisesti takaisinkytkettyä siirtorekisteriä LFSR jonka pituus on 4 ja takaisinkytkentäpolynomi on $x^4 + x^3 + x^2 + x + 1$.

   a) Määritä tämän LFSR:n generoimien jonojen jaksot.

   b) Tarkastellaan jonosalausmenetelmää jossa salausjono muodostuu tämän siirtorekisterin tuotebiteistä. Salakielijonon 19 ensimmäistä bittiä ovat

   `1 1 1 1 1 1 0 1 0 0 0 0 0 0 1 1 1 0 1`.

   Lisäksi on annettu vastaavan selkokielijonon 16. -19. bitit jotka ovat

   `0 1 0 0`.

   Määritä LFSR:n alkutila, siis salausjonon neljä ensimmäistä bittiä.

2. (6 pist.) Oletetaan että $\mathbf{X}_1$ ja $\mathbf{X}_2$ ovat riippumattomia joukossa $\{0, 1\}$ määriteltyjä satunnaismuuttujia. Merkitään symbolilla ϵ_i muuttujan $\mathbf{X}_i$ poikkeamaa (bias), kun $i = 1, 2$. Osoita että jos tällöin satunnaismuuttujat $\mathbf{X}_1$ ja $\mathbf{X}_1 \oplus \mathbf{X}_2$ ovat riippumattomia, niin $\epsilon_2 = 0$ tai $\epsilon_1 = \pm\frac{1}{2}$.

3. (6 pist.) Alkuluvun p sanotaan olevan *turvallinen alkuluku* jos $(p-1)/2$ on alkuluku.

   a) Olkoon p turvallinen alkuluku. Siis $p = 2q + 1$ missä q on alkuluku. Osoita että kunnan $\mathbb{Z}_p$ alkion multiplikatiivinen kertaluku on q silloin ja vain silloin kun se on neliönjäännös ja erisuuri kuin 1 modulo p.

   b) Kokonaisluku 08012003 (joka on sama kuin tämän tentin päivämäärä) on turvallinen alkuluku, sillä 4006001 on alkuluku. Muodosta jokin kunnan $\mathbb{Z}_{8012003}$ alkio jonka multiplikatiivinen kertaluku on 4006001.

4. (6 pist.) Tiedetään että

   $$2^{120} \equiv 15068 (\mathrm{mod} 122183).$$

   Yritä jakaa luku 122183 tekijöihin $p - 1$ menetelmää käyttäen.

5. (6 pist.) Tarkastellaan *ElGamal Julkisen Avaimen Salausmenetelmää* äärellisessä kunnassa $\mathbb{Z}_2[x]/(x^3 + x + 1)$. Salainen avain on $a = 3$ ja primitiivinen alkio on $\alpha =$ `010`. Laske vastaava julkinen avain β, ja tulkitse tällä julkisella avaimella salattu viesti $(\mathtt{110}, \mathtt{110})$.