T-79.503 Kryptologian perusteet
Tentti
11.1.2005

1. (6p.) Tarkastellaan kahta lineaarisesti takaisinkytkettyä siirtorekisteriä (LFSR), jotka on määritelty polynomeilla $f(x) = x^3 + x^2 + x + 1$ ja $g(x) = x^4 + x + 1$. Alustetaan ensimmäinen rekisteri arvolla 111, ja toinen arvolla 0101. Rekistereitä siirretään vasemmalle. Tarkastellaan rekistereiden generoimien jonojen summajonoa, joka muodostetaan laskemalla jonot yhteen termeittäin modulo 2. Mikä on se yksikäsitteisesti määrätty lyhin LFSR, joka generoi tämän summajonon?

2. Tarkastellaan "kynnysfunktiota" t: $(\mathbb{Z}_2)^3 \to \mathbb{Z}_2$, $t(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3$, missä bittioperaatiot ovat tavalliset modulo 2 yhteen- ja kertolasku.

   (a) (3p.) Muodosta funktion t differenssijakaumataulukon $N_D(a', b')$, arvot kun $a' = 010$ ja $a' = 111$ sekä kun $b' = 0$ ja $b' = 1$.

   (b) (3p.) Osoita että t säilyttää komplementoinnin, toisin sanoen, että kun syötteen jokainen bitti komplementoidaan niin funktion arvo aina komplementoituu.

3. (6p.) Määritä kokonaisluvun 2005^{2005} kolme vähiten merkitsevää numeroa kymmenjärjestelmässä.

4. (6p.)

   (a) Laske Jacobi symbolin

   $$\left(\frac{801}{2005}\right)$$

   arvo. Et saa käyttää muuta tekijöihin jakamista kuin kakkosella tai kakkosen potensseilla jakamista.

   (b) Osoita että 2005 on Eulerin pseudo-alkuluku kannan 801 suhteen.

5. (6p.) Olkoon $n = 400271$ moduuli ja $b = 117353$ julkinen eksponentti *RSA Salaamismenetelmässä*. Yritä jakaa n tekijöihin Wienerin algoritmilla. Jos onnistut, niin mitkä ovat salainen eksponentti ja $\phi(n)$.