T-110.503 Kryptologian perusteet
Tentti
9.5.2003

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) Osoita että tämän LFSR:n generoimien jonojen jaksot ovat 1 tai 5.

   b) Tarkastellaan jonosalaamismenetelmää, jossa selkokielijono salataan siirtorekisterin tuottamalla jonolla. Salakielijonon 19 ensimmäistä bittiä ovat

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

   Lisäksi on annettu vastaavan selkokielijonon 16. -19. bitit jotka ovat `0 0 0 0`. Tulkitse salakielijono.

2. Tarkastellaan salaamismenetelmää missä $\mathcal{P} = \{A, B\}$, $\mathcal{C} = \{a, b, c\}$, $\mathcal{K} = \{1, 2, 3, 4\}$, ja salaamisfunktiot e_K on määritelty seuraavasti:

K	$e_K(A)$	$e_K(B)$
1	a	b
2	b	c
3	b	a
4	c	a

   Oletetaan että avaimet valitaan yhtä suurilla todennäköisyyksillä.

   a) (3 pist.) Osoita että

   $$\mathbf{Pr}[\mathbf{x} = A | \mathbf{y} = b] = \frac{2\mathbf{Pr}[\mathbf{x} = A]}{1 + \mathbf{Pr}[\mathbf{x} = A]}.$$

   b) (3 pist.) Onko salaamismenetelmä täydellisesti salaava?

3. Olkoon $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$. Tarkastellaan S-boxia, jolla on kolme syötebittiä ja kolme tuotosbittiä, ja joka on määritelty funktiolla $\pi_S(w) = w^3$, $w \in \mathbb{F}$. Esimerkiksi $\pi_S(\mathtt{011}) = \pi_S(x + 1) = (x + 1)^3 = x^3 + x^2 + x + 1 = x^2 = \mathtt{100}$.

   a) (3 pist.) Olkoon $a' = \mathtt{100} = x^2$. Osoita että

   $$\pi_S(w + a') + \pi(w) = x^2 w^2 + (x^2 + x)w + x^2 + 1, \text{ kaikilla } w \in \mathbb{F}.$$

   b) (3 pist.) Laske S-boxin π_S differenssijakaumataulun (*Difference Distribution Table*) rivi syöte-erotuksella $a' = \mathtt{100}$. Huomaa että a)-kohdasta voisi olla hyötyä.

4. (6 pist.) Tarkastellaan alkulukua $p = 2003$. Muodosta joku kertalukua $q = 11$ oleva alkio multiplikatiivisessa ryhmässä $\mathbb{Z}^*_{2003}$.

5. (6 pist.) Olkoon RSA menetelmän julkinen avain (n, b), missä $n = 355044523$ ja $b = 311711321$. Yritä jakaa n tekijöihin Wienerin Algoritmilla.