T-79.503 Kryptologian perusteet
Tentti
26.04.2004

1. (6 pist) 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?

2. (6 pist) Olkoon $f(x)$ polynomi, jonka aste on n, missä n on positiivinen kokonaisluku. Tarkastellaan Galois'n kuntaa $GF(2^n) = \mathbb{Z}_2[x]/f(x)$ ja siinä määriteltyä kuvausta $z \mapsto z^3$. Osoita että tämä kuvaus on melkein täydellisesti epälineaarinen, eli että tämän kuvauksen määrittelemän S-boxin differenssijakaumataulukossa $N_D(a', b')$ kaikki arvot ovat joko 0 tai 2.

3. Onko seuraavilla kongruenssiyhtälöillä ratkaisuja? Jos on niin määritä ne.

   a) (3 pist) $x^4 \equiv 26 \,(\mathrm{mod} 2004)$

   b) (3 pist) $26x \equiv 4 \,(\mathrm{mod} 2004)$

4. (6 pist) Alice käyttää RSA salaamismenetelmää ja hänen RSA moduulinsa on $n = 334501 = 167 \cdot 2003$. Tulkitse salakieliteksti $y = 2004$.

5. (6 pist) Ratkaise kongruenssiyhtälö

$$3^x \equiv 24 (\mathrm{mod}\, 31)$$

   käyttämällä Shanksin algoritmia.