T-79.503 [vanha: T-110.503] Kryptologian perusteet
Tentti
03.09.2003

1. (6 pist.) Tarkastellaan kolmen kierroksen Feistel salaajaa, joka on määritelty seuraavasti. Olkoon lohkon pituus $2n$ ja selväkieli (L_0, R_0), missä L_0 ja R_0 ovat kumpikin n:n bitin lohkoja. Lasketaan

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f_i(R_{i-1}), \end{aligned}$$

missä f_i on n:n bitin funktio ja $i = 1, 2, 3$. Salakieli on (L_3, R_3). Tutki, miten funktiot f_1, f_2 ja f_3 on valittava, jotta tämä Feistel salaaja olisi identtinen kuvaus, eli $L_0 = L_3$ ja $R_0 = R_3$ aina.

2. (6 pist.) Oletetaan että AES lohkosalaamismenetelmää käytetään CBC käyttötavalla.

   a) Kuinka monta salakielilohkoa arviolta tarvitaan jotta todennäköisyys sille että löytyy kaksi samaa salakielilohkoa on suurempi kuin 0.5?

   b) Oletetaan että löytyy kaksi samanlaista salakielilohkoa, jotka on muodostettu samalla avaimella (ja CBC käyttötavalla). Mitä voidaan sanoa näitä salakielilohkoja vastaavista selväkielilohkoista?

3. (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), $\epsilon_i = Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, 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 $\epsilon_1 = \pm\frac{1}{2}$.

4. (6 pist.) Ratkaise kongruenssiyhtälö

$$x^3 \equiv 9 \,(\mathrm{mod} 2003).$$

5. (6 pist.) Alice käyttää RSA salaamismenetelmää ja hänen RSA moduulinsa on $n = 334501 = 167 \cdot 2003$. Tulkitse salakieliteksti $y = 2003$.