T-79.503 [vanha T-110.503] Kryptologian perusteet
Tentti
15.12.2003

1. Tarkastellaan jonosalainta, jonka salausjono $z_1, z_2, \ldots$ muodostuu toistamalla kiinteänpituista satunnaisesti generoitua bittijonoa $K = (k_1, k_2, \ldots, k_m)$. Siis $z_j = k_i$ jos ja vain jos $j \equiv i \,(\mathrm{mod} m)$.

   a) (3 pist) Selväkielen redundanssi on R. Määritä ratkaisukynnys, eli kuinka monta bittiä salakielijonoa tarvitaan keskimäärin avaimen K yksikäsitteiseksi määrittämiseksi?

   b) (3 pist) Oletetaan nyt että $m = 5$ ja selväkieli on muodostettu toistamalla seuraavaa menettelyä: kaksi bittiä generoidaan satunnaisesti ja kolmas bitti saadaan laskemalla nämä kaksi bittiä yhteen modulo 2. Viisitoista ensimmäistä salakielibittiä ovat: 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1. Yritä määrittää avain $K = (k_1, k_2, k_3, k_4, k_5)$.

2. (6 pist) Tarkastellaan äärellistä kuntaa $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$ missä on annettu seuraava funktio $f : \mathbb{F} \to \mathbb{F}$:

$$\begin{aligned} f(z) &= z^{-1}, \text{ jos } z \neq 0, \\ f(0) &= 0. \end{aligned}$$

   Oletetaan että Feistel salaaja on määritelty seuraavasti:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} + f(R_{i-1} + K_i), \end{aligned}$$

   missä $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$ ja kierrosavaimet ovat $K_i = K^i$, kun $i = 1, 2, 3$, missä$K \in \mathbb{F}$ on avain. Oletetaan että yksi selväkieli-salakielipari tunnetaan. Siinä on $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ ja $R_3 = 100$. Yritä määrittää avain K.

3. (6 pist) Ratkaise seuraava kongruenssiyhtälösysteemi

$$\begin{aligned} 15x &\equiv 12 \,(\mathrm{mod} 2003) \\ 12 &\equiv x \,(\mathrm{mod} 2004) \end{aligned}$$

4. (6 pist) Tiedetään että

$$2^{4!} \equiv 1655213 \,(\mathrm{mod} 15122003).$$

   Käyttäen Pollardin $p-1$ algoritmia yritä löytää jokin luvun 15122003 epätriviaali tekijä.

5. (6 pist) El Gamal Allekirjoitusmenetelmässä parametrit ovat $p = 31$ ja $\alpha = 3$. Alice saa käsiinsä kaksi viestiä x_1 ja x_2 sekä niiden allekirjoitukset (γ_1, δ_1) ja (γ_2, δ_2) jotka on muodostettu samalla allekirjoitusavaimella. Nämä arvot ovat seuraavat

$$\begin{aligned} x_1 &= 25, \ \gamma_1 = 24, \ \delta_1 = 7 \\ x_2 &= 5, \ \gamma_2 = 24, \ \delta_2 = 17 \end{aligned}$$

   Pystyisitkö määrittämään salaisen allekirjoitusavaimen?