T-110.503 Kryptologian perusteet
Loppukoe
8.1.2002

1. (6 pist.) Selväkieli muodostuu viiden bitin lohkoista, joissa kaikissa ykkösiä on vähemmän kuin nollia. Jokaisen tällaisen lohkon todennäköisyys on yhtä suuri. Kuinka monta bittiä tässä selväkielessä on entropiaa lohkoa kohden?

2. (6 pist.) Olkoon annettu positiivinen kokonaisluku r ja yhdistelyfunktio $f : \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}$. Määritellään eräänlainen *Feistel salaaja* seuraavasti:

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= (L_{i-1} + f(R_{i-1}, K_i)) \bmod 26, \end{aligned}$$

   missä $K_i \in \mathbb{Z}_{26}$, $i = 1, 2, \ldots, r$, ja L_j, $R_j \in \mathbb{Z}_{26}$, $j = 0, 1, 2, \ldots, r$. Selväkieli on (L_0, R_0) ja salakieli on (L_r, R_r).

   Tarkastellaan tapausta jossa $r = 2$, avain K on tuntematon, $K_1 = K$ ja $K_2 = (K + 13) \bmod 26$, ja yhdistelyfunktio f on annettu kaavalla $f(R_{i-1}, K_i) = (R_{i-1} \times K_i) \bmod 26$.

   a) Osoita että jos valitaan selväkieleksi (1,13) niin $R_2 = K$.

   b) Valitse sellainen selväkieli, jolla saadaan $L_2 = K$.

3. (6 pist.)

   a) Esitä Solovay-Strassen alkulukutesti parittomalle positiiviselle kokonaisluvulle n, $n > 1$.

   b) Onko 21 Eulerin pseudo-alkuluku kannan 2 suhteen?

4. (6 pist.) Moduuli on $2002 = 2 \times 7 \times 11 \times 13$. Määritä kongruenssiyhtälölle

$$x^8 \equiv 1 (\mathrm{mod}\, 2002)$$

   joku epätriviaali ratkaisu, siis joku ratkaisu, joka on erisuuri kuin ± 1 modulo 2002.

5. (6 pist.) Tarkastellaan ElGamalin Julkisen Avaimen Salausmenetelmää Galois kunnassa $\mathrm{GF}(2^4)$ kun polynomina on $x^4 + x^3 + 1$ ja primitiivialkiona $\alpha = 0010 = x$. Salainen avaimesi on $a = 4$.

   a) Laske julkinen avaimesi β.

   b) Tulkitse salakieliteksti (0100,1110) salaisen avaimesi avulla. Muistathan että kun selväkieli on $X \in \mathrm{GF}(2^4)^*$ niin salakieli on $(\alpha^k, X\beta^k)$ missä kokonaisluku k on vain salaajan tiedossa.