TIK-110.503 Kryptologian perusteet
Loppukoe
7.4.2001

1. (6 pist.) Salattava selväkieli muodostuu yhtä todennäköisistä m bitin lohkoista, joissa on täsmälleen yksi 1-bitti, ja muut bitit ovat nollia.

   a) Määritä tämän selväkielen suhteellinen redundanssi.

   b) Tätä selväkieltä salataan salausmenetelmällä, missä $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = 2^m$. Osoita, että yksikäsitteisyysväli $n_0 \leq 2$ kaikilla positiivisilla kokonaisluvuilla m paitsi kun $m = 3$. (Opastus: $\log_2 3 \approx 1.585$.)

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 $r = 2$, $K_1 = K_2 = K$, ja yhdistelyfunktio f on annettu kaavalla $f(X, K) = (X \times K) \bmod 26$. Olkoon nyt selväkieli (17,13) ja sitä vastaava salakieli (4,13). Määrää avain K.

3. (6 pist.) Olkoon $n = pq$, missä p ja q ovat alkulukuja. Voimme olettaa, että $p > q > 2$ ja merkitsemme erotusta $p - q$ symbolilla d. Huomaa, että silloin d on positiivinen ja parillinen.

   a) Oletetaan nyt, että n ja d tunnetaan. Näytä miten p ja q voidaan laskea.

   b) Jos n on annettu, ja lisäksi tiedetään, että d on pieni, niin voidaan kokeilla läpi kaikki d:n mahdolliset arvot ja laskea a-kohdassa mainitulla tavalla p ja q. Käytä tätä menetelmää luvun 4003997 jakamiseksi tekijöihin.

4. (6 pist.) Moduuli on $2001 = 3 \times 23 \times 29$. Onko kongruenssiyhtälöllä

   $$x^4 \equiv 7 (\mathrm{mod}\, 2001)$$

   kokonaislukuratkaisuja x?

5. (6 pist.) Tarkastellaan ElGamal salausmenetelmää Galois kunnassa $\mathrm{GF}(2^4)$, jossa polynomi on $x^4 + x + 1$ ja primitiivinen alkio $\alpha = 0010 = x$. Sinun yksityinen salainen avaimesi on $a = 7$.

   a) Laske julkinen avaimesi β.

   b) Tulkitse salakieli (0100,1110) käyttäen salaista avaintasi. Muista että kun selväkieli on X niin salakieli lasketaan käyttäen kaavaa $(\alpha^k, X\beta^k)$, missä kokonaisluku k on ainoastaan salaajan tiedossa.