TIK-110.503 Kryptologian perusteet
Loppukoe
4.9.2001

1. (6 pist.) Tarkastellaan lineaarisesti takaisinkytkettyä siirtorekisteriä kytkentäpolynomilla $x^4 + x^3 + x^2 + x + 1$.

   a) Määritä tämän LFSRn generoimien bittijonojen jaksot.

   b) Tarkastellaan tähän LFSRään perustuvaa jonosalaajaa. Eräs salakieliteksti on

   1 1 1 0 1 1 0 1 1 1 1 1 0 0 0 1 0

   ja tiedetään että sitä vastaavaan selväkielijonon 4. ja 12. bitti on **0** ja 8. ja 16. bitti on **1**. Määritä rekisterin alkutila, siis salausjonon neljä ensimmäistä bittiä.

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 $2001 = 3 \times 23 \times 29$. Onko kongruenssiyhtälöllä

$$x^4 \equiv 9 (\bmod\, 2001)$$

   kokonaislukuratkaisuja x?

5. (6 pist.) Tarkastellaan seuraavaa El Gamal allekirjoitusmenetelmän muunnosta Galois kunnassa. Julkiset parametrit ovat n, q ja α, missä q on luvun $2^n - 1$ tekijä ja α on kunnassa $GF(2^n)$ kertalukua q oleva alkio. Käyttäjän salainen avain on $a \in \mathbb{Z}_q$ ja julkinen avain on $\beta = \alpha^a$. Muodostaessaan allekirjoituksen viestille x käyttäjä generoi ensin salaisen luvun $k \in \mathbb{Z}_q^*$ ja laskee allekirjoituksen (γ, δ) seuraavasti:

$$\begin{aligned} \gamma &= \alpha^k \text{ (kunnassa } GF(2^n)) \\ \delta &= (x - a\gamma')k^{-1} \bmod q, \end{aligned}$$

   missä γ' on kunnan alkion (bittijonon) γ esitys kokonaislukuna. Oletetaan että Bob käyttää tätä menetelmää ja kahden viestin x_1 ja x_2 allekirjoitukset ovat (γ_1, δ_1) ja (γ_2, δ_2), vastaavasti. Alice näkee viestit ja niiden allekirjoitukset ja huomaa että $\gamma_1 = \gamma_2$.

   a) Kuvaa miten Alice voi nyt johtaa tietoa Bobin salaisesta avaimesta.

   b) Olkoon $n = 8$, $q = 15$, $x_1 = 1$, $x_2 = 4$, $\delta_1 = 11$, $\delta_2 = 2$, ja $\gamma_1' = \gamma_2' = 7$. Mitä Alice voi nyt sanoa Bobin salaisesta avaimesta?