TIK-110.503 Kryptologian perusteet
Loppukoe
12.01.2001

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 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.) DES salausmenetelmän avaimet ovat 64 bitin jonoja, joissa joka 8. bitti on tarkistusbitti, joka lasketaan sitä edeltävän seitsemän bitin summana modulo 2. Avaintenhallintakeskus käyttää DES salausmenetelmää ja yhtä DES-avainta, nk. "master"-avainta, kun se salaa DES avaimia lähetettäväksi loppukäyttäjille. Jokainen salakielilohko sisältää siis yhden salatun DES avaimen. Arvioi tämän menetelmän ratkaisukynnystä, eli siis kuinka monta salakielilohkoa keskimäärin tarvitaan master-avaimen yksikäsitteiseksi määrittämiseksi olettaen että tarvittavaa laskentakapasiteettia on riittävästi.

3. (6 pist.) SHA-1 hashfunktion määrittelyssä käytetään funktiota T joka on annettu seuraavasti. Olkoon X_0, X_1 ja X_2 kolme 32 bitin jonoa. Silloin $T(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$, missä $\wedge$ on biteittäin suoritettu "and" kertolasku, ja $\vee$ on biteittäin suoritettu "or" yhteenlasku. Olkoon $t(x_0, x_1, x_2)$ Boolen funktio, joka on funktion T yhden ulostulobitin muodostama komponentti.

   a) Määritä Boolen funktion t algebrallinen normaalimuoto.

   b) Kolmen muuttujan Boolen funktion f *linearinen struktuuri* on vektori $w = (w_1, w_2, w_3) \neq (0, 0, 0)$ jolle pätee että $f(x \oplus w) \oplus f(x)$ on vakio. Osoita että Boolen funktiolla t on täsmälleen yksi lineaarinen struktuuri.

4. (6 pist.) Todista että konruenssiyhtälöllä

   $$x^{12} \equiv x^1 (\mathrm{mod}\, 2001)$$

   on epätriviaaleja ($\neq 0$ tai 1) ratkaisuja. (Opastus: $2001 = 3 \times 23 \times 29$.)

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?