TIK-110.503 Kryptologian perusteet
Loppukoe
16.12.1999

1. (6 pist.) Salausmenetelmänä on DES lohkosalausalgoritmi. Selväkielidata koostuu neljän bitin lohkoista, joissa kussakin on täsmälleen yksi 1-bitti ja muut kolme bittiä ovat nollia.

   a) Selväkieltä salataan sellaisenaan. Määrää ratkaisukynnyksen pituus (bitteinä).

   b) Ennen salausta selväkielen joka neljännen bitin jälkeen lisätään neljä satunnaisbittiä. Määrää nyt salausmenetelmän ratkaisukynnys.

2. (6 pist.) Tarkastellaan Feistelin salaajaa, jonka i. kierros määritellään seuraavasti:

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

   missä K_i on kierrosavain ja F_i on kierrosfunktio. Annetulle bittijonolle A merkitään symbolilla $c(A)$ bittijonoa, joka saadaan kun A:n jokainen bitti komplementoidaan, siis esim. kun $A = 001$, niin $c(A) = 110$. Olkoon $Y = (L_r, R_r)$ salakielidata, joka on saatu salaamalla selväkielidata $X = (L_0, R_0)$ (= bittijonot L_0 ja R_0 pantuna peräkkäin) r kierroksen Feistel-salaajalla, jonka kierrosavaimet ovat $K_1, K_2, \ldots, K_r$. Osoita että on olemassa sellaiset kierrosavaimet, että selväkieltä $c(X)$ vastaava salakieli on $c(Y)$.

3. a) (3 pist.) Osoita, että 12 ei ole neliöjäännös modulo 1999.

   b) (3 pist.) Osoita, että kongruenssiyhtälöllä

$$16^x \equiv 12 (\mathrm{mod} 1999)$$

   ei ole ratkaisua.

4. (6 pist.) Bob ja Bart käyttävät Rabinin salausmenetelmää. Bobin moduli on $n_1 = 2183$ ja Bartin moduli on $n_2 = 2173$. Kummallakin on $B = 0$. Alice salaa erään luvun x, $0 < x < 2173$, heille molemmille, ja lähettää Bobille salakielitekstin $y_1 = 1111$ ja Bartille $y_2 = 2027$. Ratkaise x. (Sillä että modulien kaikki alkutekijät eivät ole kongruentteja luvun 3 kanssa modulo 4, ei ole ratkaisun kannalta merkitystä.)

5. (6 pist.) Tarkastellaan Galois kuntaa $GF(2^4)$ polynomilla $x^4 + x + 1$. Muodosta multiplikatiivisen ryhmän $GF(2^4)^*$ aidot sykliset aliryhmät, siis sykliset aliryhmät, joissa on vähemmän kuin 15 alkiota.