T-110.503 Kryptologian perusteet
Tentti
4.9.2002

1. (6 pist.) Salausmenetelmän avain on 100 bittinen. Avainten tuottamiseen käytetään satunnaislukugeneraattoria, joka generoi viisi bittiä kerrallaan. Generaattorissa on vika, josta johtuen se pystyy tuottamaan vain sellaisia viiden bitin lohkoja, joissa ykkösiä on vähemmän kuin nollia. Jokaisen tällaisen lohkon todennäköisyys on yhtä suuri. Kuinka monta bittiä tuotetuissa avaimissa on entropiaa, eli mikä on efektiivinen avaimen pituus?

2. (6 pist.) Tarkastellaan kolmen kierroksen Feistel salaajaa, joka on määritelty seuraavasti. Olkoon lohkon pituus $2n$ ja selväkieli (L_0, R_0), missä L_0 ja R_0 ovat kumpikin n:n bitin lohkoja. Lasketaan

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

missä f_i on n:n bitin funktio ja $i = 1, 2, 3$. Salakieli on (L_3, R_3). Tutki, milloin tämä Feistel salaaja on identtinen kuvaus, eli milloin on aina $L_0 = L_3$ ja $R_0 = R_3$.

3. (6 pist.) Olkoon $n = pq$, missä p ja q ovat alkulukuja. Voimme olettaa, että $p > q > 2$ ja merkitsemme $d = \frac{p-q}{2}$ ja $x = \frac{p+q}{2}$. Silloin siis $n = x^2 - d^2$. Osoita että jos $d < \sqrt{p+q}$ niin x voidaan laskea määrittämällä luvun n neliöjuuri pyöristettynä lähimpään suurempaan kokonaislukuun.

   [Jos sinulla on laskin käytässäsi voit jakaa luvun $n = 4007923$ tekijöihin tällä menetelmällä.]

4. (6 pist.) Moduuli on $2002 = 2 \times 7 \times 11 \times 13$. Ratkaise toinen seuraavista tehtävistä. Valinta on sinun, siis joko a) tai b).

   a) Kuinka monta ratkaisua x on kongruenssiyhtälöllä

   $$x^4 \equiv 9 \pmod{2002}$$

   b) Kuinka monta ratkaisua x on kongruenssiyhtälöllä

   $$x^9 \equiv 4 \pmod{2002}$$

5. (6 pist.) Kuvaa pääpiirteittäin miten RSA salausmenetelmän avaimet muodostetaan, ja miten salaaminen ja tulkinta RSA menetelmässä tapahtuu.