T-110.503 Kryptologian perusteet
Loppukoe
4.3.2002

1. (6 pist.) Selväkieli muodostuu kahdeksan bitin lohkoista, joissa kaikissa ykkösiä on (aidosti) vähemmän kuin nollia. Jokaisen tällaisen lohkon todennäköisyys on yhtä suuri. Kuinka monta bittiä tässä selväkielessä on entropiaa lohkoa kohden?

2. (6 pist.) 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. Tarkastellaan SHA-1 hashfunktion määrittelyssä käytettyä Boolen funktiota $t(x_1, x_2, x_3)$, jonka algebrallinen normaalimuoto on $t(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$. Osoita että Boolen funktiolla t on täsmälleen yksi lineaarinen struktuuri.

3. (6 pist.) Olkoon $n = pq$, missä p ja q ovat alkulukuja. Voidaan olettaa, että $p > q > 2$ ja merkitään erotusta $p - q$ symbolilla d. Huomataan, 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 $2002 = 2 \times 7 \times 11 \times 13$. Onko kongruenssiyhtälöllä

   $$x^4 \equiv 3 (\mathrm{mod}\ 2002)$$

   ratkaisuja?

5. (6 pist.) Tarkastellaan *ElGamalin julkisen avaimen salausmenetelmää* Galois kunnassa $\mathrm{GF}(2^4)$ kun polynomina on x^4+x+1 ja primitiivialkiona $\alpha = 0010 = x$. Salainen avaimesi on $a = 4$.

   a) Laske julkinen avaimesi β.

   b) Tulkitse salakieliteksti (0100,1110) salaisen avaimesi avulla. Muistetaan että kun selväkieli on $X \in \mathrm{GF}(2^4)^*$ niin salakieli on $(\alpha^k, X\beta^k)$ missä kokonaisluku k on vain salaajan tiedossa.