TIK-110.503 Kryptologian perusteet
Loppukoe
5.9.2000

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

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 $X = (L_0, R_0)$ (= bittijonojen L_0 ja R_0 katenaatio) r kierroksen Feistel-salaajalla, jonka kierrosavaimet ovat $K_1, K_2, \ldots, K_r$. Osoita, että kun selväkieli $c(X)$ salataan tällä Feistel-salaajalla käyttäen kierrosavaimia $c(K_1), c(K_2), \ldots, c(K_r)$ niin salakieli on $c(Y)$.

3. (6 pist.) Ratkaise kongruenssiyhtälöryhmä

$$\begin{aligned} 3x + 7y &\equiv 0 (\mathrm{mod} 42) \\ 2x - 3y &\equiv 2 (\mathrm{mod} 42). \end{aligned}$$

4. (6 pist.) Luku 59 on luvun 1481 neliöjuuri modulo 2000. Määrää joku toinen luku joka on luvun 1481 neliöjuuri modulo 2000. Opastus: Jos m_1 jakaa luvun $a - b$ ja m_2 jakaa luvun $a + b$, ja jos $\gcd(m_1, m_2) = 1$, niin $a^2 \equiv b^2 \pmod{m_1 m_2}$.

5. (6 pist.) Tarkastellaan ElGamalin Julkisen Avaimen Salausmenetelmää Galois kunnassa $\mathrm{GF}(2^4)$ kun polynomina on $x^4 + x^3 + 1$ ja primitiivialkiona $\alpha = 0010 = x$. Salainen avaimesi on $a = 4$.

   a) Laske julkinen avaimesi β.

   b) Tulkitse salakieliteksti (0100,1110) salaisen avaimesi avulla. Muistathan 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.