T-79.5501 Cryptology
First midterm exam
March 9th, 2007
Each problem is worth 6 points.
Suomenkielinen koe toisella puolella.

1. The length of the key of a cryptographic system is 100 bits. Key generation is performed using a pseudorandom number generator which generates the key in blocks of five bits. The generator is flawed in such a way that it only produces five bit blocks where the number of ones is less than the number of zeroes. Every such block occurs with equal probability. What is the actual strength of the key produced by this generator, that is, how many bits of entropy the key has? Compare this with the maximum entropy of a string of 100 bits.

2. Consider two binary linear feedback shift registers with polynomials $f(x) = x^3 + x^2 + x + 1$ and $g(x) = x^4 + x + 1$. Initialize the first register with 111, and the second one with 0101 (the registers are shifted to left). Generate the two output sequences and take their xor-sum sequence. Determine the unique shortest linear feedback shift register that generates the sum-sequence. Explain why this register is unique.

3. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$ and let $f : \mathbb{F} \to \mathbb{F}$ be a function defined as

$$\begin{aligned} f(z) &= z^{-1}, \text{ for } z \neq 0, \\ f(0) &= 0. \end{aligned}$$

   Let a Feistel cipher be defined as follows

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

   where $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$ and the round keys are defined as $K_i = K^i$, for $i = 1, 2, 3$, where $K \in \mathbb{F}$ is the key. Assume that one known plaintext-ciphertext pair is given as follows: $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ and $R_3 = 100$. Find the key $K$.

4. Suppose that $\mathbf{X}_1, \mathbf{X}_2$ and $\mathbf{X}_3$ are independent random variables defined on the set $\{0, 1\}$. Let $\epsilon_i$ denote the bias of $\mathbf{X}_i$, for $i = 1, 2, 3$. Prove that if the random variables $\mathbf{X}_1 \oplus \mathbf{X}_2$ and $\mathbf{X}_2 \oplus \mathbf{X}_3$ are independent, then $\epsilon_1 = 0$ or $\epsilon_3 = 0$ or $\epsilon_2 = \pm\frac{1}{2}$.

T-79.5501 Kryptologia
Ensimmäinen välikoe
9.3.2007
Jokaisesta tehtävästä saa 6 pistettä.
English text on the other side.

1. Salausjärjestelmän avaimen pituus on 100 bittiä. Avain luodaan pseudosatunnaislukugeneraattorilla, joka tuottaa luvun viiden (5) bitin lohkoissa. Generaattori on viallinen, joten se tuottaa viisibittisiä lohkoja, joissa jokaisessa on vähemmän ykkösiä kuin nollia. Jokainen tällainen lohko esiintyy yhtä suurella todennäköisyydellä. Mikä on tämän generaattorin tuottamien avainten todellinen vahvuus, ts. kuinka monta bittiä entropiaa avaimella on? Vertaa tulostasi 100-bittisen bittijonon maksimientropiaan.

2. Tarkastellaan kahta lineaarisesti takaisinkytkettyä siirtorekisteriä (LFSR), jotka on määritelty polynomeilla $f(x) = x^3 + x^2 + x + 1$ ja $g(x) = x^4 + x + 1$. Alustetaan ensimmäinen rekisteri arvolla 111 ja toinen arvolla 0101. (Rekistereitä siirretään vasemmalle.) Muodosta jonot ja laske niiden xor-summajono. Mikä on se yksikäsitteisesti määrätty lyhin LFSR, joka generoi tämän summajonon? Perustele tämän rekisterin yksikäsitteisyys.

3. Tarkastellaan äärellistä kuntaa $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$ ja olkoon funktio $f : \mathbb{F} \to \mathbb{F}$ määritelty

$$\begin{aligned} f(z) &= z^{-1}, \text{ for } z \neq 0, \\ f(0) &= 0. \end{aligned}$$

   Määritellään Feistelin salain seuraavasti:

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

   missä $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$. Edelleen kierrosavaimet (round keys) ovat $K_i = K^i$, missä $i = 1, 2, 3$, ja $K \in \mathbb{F}$ on avain. Oletetaan, että tunnetaan seuraavanlainen selväkieli-salakieli pari: $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ and $R_3 = 100$. Määritä avain $K$.

4. Olkoon $\mathbf{X}_1, \mathbf{X}_2$ ja $\mathbf{X}_3$ riippumattomia satunnaismuuttujia arvojoukossa $\{0, 1\}$. Merkitään symbolilla $\epsilon_i$ satunnaismuuttujan $\mathbf{X}_i$ suuntaumaa (bias), kun $i = 1, 2, 3$. Osoita, että jos satunnaismuuttujat $\mathbf{X}_1 \oplus \mathbf{X}_2$ ja $\mathbf{X}_2 \oplus \mathbf{X}_3$ ovat riippumattomia, niin silloin $\epsilon_1 = 0$ tai $\epsilon_3 = 0$ tai $\epsilon_2 = \pm\frac{1}{2}$.