T-79.5501 Cryptology
Midterm Exam 1
Friday, February 19, 2016

1. (6 pts) Let n be a positive integer. A *Latin square* of order n is a $n \times n$ array L of the integers $1, 2, \ldots, n$ such that each of the n integers occurs exactly once in each row and each column of L. We denote by $L(i, j)$ the element in the i'th row and j'th column of L.

   An example of a Latin square of order 3 is as follows.

1	2	3
3	1	2
2	3	1

   Given any Latin square L of order n, we can define a cryptosystem where $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, 2, \ldots, n\}$, and

   $$e_i(j) = L(i, j), \text{ for all } i \in \mathcal{K} \text{ and } j \in \mathcal{P}.$$

   Prove that this *Latin Square Cryptosystem* achieves perfect secrecy if every key is used with equal probability.

2. (6 pts) Recall that for a connection polynomial $f(x)$ of a binary LFSR we have that $(f^*)^* = f$ and $\Omega(f)$ is the set of binary sequences generated using this LFSR. Further, we know that $\Omega(f)$ can also be expressed as a set of quotients of the form $P(x)/f^*(x)$, where $\deg(P(x)) < \deg(f(x))$.

   Now, let $f(x)$ and $g(x)$ be two connection polynomials of binary LFSRs. Give the proof of the following result: If $\Omega(f) \subset \Omega(g)$, then $f(x)$ divides $g(x)$.

3. The *Autokey cipher* over the alphabet $\mathbb{Z}_{26}$ is defined as follows. Given a key $(k_1, k_2, \ldots, k_m)$, where $m \geq 1$, the plaintext $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{26}^n$, $n \geq m$ is encrypted to ciphertext $y = (y_1, \ldots, y_n)$ as follows

   $$\begin{aligned} y_i &= x_i + k_i \bmod 26, \text{ for } i = 1, 2, \ldots, m, \text{ and} \\ y_i &= x_i + x_{i-m} \bmod 26, \text{ for } i = m+1, m+2, \ldots, n. \end{aligned}$$

   (a) (3 pts) The attacker sees the ciphertext, and transforms it to sequence $z = (z_1, \ldots, z_n)$ as follows:

   $$\begin{aligned} z_i &= y_i, \text{ for } i = 1, 2, \ldots, m, \text{ and} \\ z_i &= y_i - z_{i-m} \bmod 26, \text{ for } i = m+1, m+2, \ldots, n. \end{aligned}$$

   Show that then z is equal to the ciphertext obtained by encrypting x using the $2m$-periodic Vigenère cipher with keyword $(k_1, \ldots, k_m, -k_1, -k_2, \ldots, -k_m)$.

   (b) (3 pts) Suppose the length m of the key of the autokey cipher is secret. Explain how the attacker can apply the *Index of Coincidence* method for finding m.

4. (6 pts) Suppose that $\mathbf{T}_1$ and $\mathbf{T}_2$ are independent random variables which take on values from the set $\{0, 1\}$. We use c_i to denote the correlation of $\mathbf{T}_i$, $c_i = 2\Pr[\mathbf{T}_i = 0] - 1$, for $i = 1, 2$. Suppose that $c_1 = c_2 = 1/3$. Show that then the random variables $\mathbf{T}_1$ and $\mathbf{T}_1 \oplus \mathbf{T}_2$ are not independent.

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.