T-79.5501 Cryptology
Midterm Exam 1
March 9, 2012

1. (6 pts) Suppose that in a cryptosystem the following holds: for each pair (x, y), $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there is exactly one key $K \in \mathcal{K}$ such that $e_K(x) = y$, that is, $H(\mathbf{K}|\mathbf{PC}) = 0$. Prove that then the cryptosystem achieves perfect secrecy if and only if $H(\mathbf{K}) = H(\mathbf{C})$.

2. (6 pts) Let $f(x)$ be a feedback polynomial of a binary LFSR. Then $(f^*)^* = f$ and $\Omega(f)$ is the set of binary sequences generated using this LFSR.

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

3. (6 pts) A *linear structure* of a Boolean function g of n variables is defined as a non-zero vector w of length n such that $g(x \oplus w) \oplus g(x)$ is constant. Consider the Geffe function $g(x) = g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_3$. Show that g has exactly one linear structure.

4. (6 pts) Let $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ be independent random variables with biases $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1/4$. Show that then $\mathbf{T}_1 \oplus \mathbf{T}_2$ and $\mathbf{T}_2 \oplus \mathbf{T}_3$ are not independent random variables.

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