T-79.5501 Cryptology
Midterm Exam 1
March 7, 2011

1. Let us consider a cryptosystem which achieves perfect secrecy and suppose that $\mathbf{Pr}[y] > 0$, for all $y \in \mathcal{C}$. For such a cryptosystem, prove the following statements.

   (a) (3 pts) If 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 $e_K(x) = y$, then $H(\mathbf{K}) = H(\mathbf{C})$.

   (b) (3 pts) If $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$, then every ciphertext has equal probability.

2. Let us consider two binary linear feedback shift registers with connection polynomials $f(x) = x^4 + x^3 + x^2 + 1$ and $g(x) = x^3 + x + 1$, where $g(x)$ is primitive.

   (a) (3 pts) Determine $\mathrm{lcm}(f(x), g(x))$.

   (b) (3 pts) Let S_1 be a sequence generated by the LFSR with polynomial $f(x)$ and S_2 be a sequence generated by the LFSR with polynomial $g(x)$. What is the longest period of the sum sequence $S_1 + S_2$ (termwise mod 2)? Show how it can be achieved.

3. (6 pts) Given three input bits (x_1, x_2, x_3) the output bits (y_1, y_2) of an S-box, which maps three bits to two bits, are defined as follows:

$$\begin{aligned} y_1 &= x_1x_2 \oplus x_3 \\ y_2 &= x_1x_3 \oplus x_2. \end{aligned}$$

   Determine the output bit y_j for which the bias of $x_1 \oplus x_2 \oplus y_j$ is different from zero.

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.