T-79.5501 Cryptology
Midterm Exam 1
March 11, 2008

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) Solve the following system of congruences

$$\begin{aligned} 11x &\equiv 3 \pmod{2008} \\ 3x &\equiv 0 \pmod{2007}. \end{aligned}$$

3. Let us consider two binary linear feedback shift registers with connection polynomials $f(x) = x^4 + x^3 + x^2 + 1$ and $g(x) = x^3 + x^2 + 1$, 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 $g(x)$. Determine the largest possible period of the sum sequence $S_1 + S_2$ (termwise mod 2).

4. (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.