T-79.5501 Cryptology
EXAM
Friday, October 29, 2010

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 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 $g(x) = g(x_1, x_2, x_3) = x_0x_1 \oplus x_0x_2 \oplus x_2$. Show that g has exactly one linear structure.

4. (6 pts) Bob and Bart are using the Rabin Cryptosystem. Bob's modulus is 2183 and Bart's modulus is 2279. Alice wants to send an integer x, $0 < x < 2183$, encrypted to both of them. She sends ciphertext 1479 to Bob and the ciphertext 418 to Bart. Carol sees the ciphertexts and she knows Bob's and Bart's moduli. Show how Carol can compute x without factoring of moduli. Hint: Use Chinese Remainder Theorem.

5. (6 pts) Element $\alpha = 1639$ is of order 14 in the multiplicative group $\mathbb{Z}^*_{2009}$. It is given that the element $\beta = 862$ is in the subgroup generated by α. Using Shanks' algorithm compute the discrete logarithm x of $\beta = 862$ to the base $\alpha = 1639$, that is, solve the equation

$$1639^x \equiv 862 \,(\mathrm{mod}\, 2009).$$

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