T-79.503 Foundations of Cryptology
Exam
January 11, 2005

1. (6p.) Consider two binary linear feedback shift registers with polynomials $f(x) = x^3 + x^2 + x + 1$ and $g(x) = x^4 + x + 1$. Initialize the first register with 111, and the second one with 0101 (the registers are shifted to left). Generate the two output sequences and take their xor-sum sequence. Determine the unique shortest linear feedback shift register that generates the sum-sequence.

2. Consider the "threshold function" t: $(\mathbb{Z}_2)^3 \to \mathbb{Z}_2$, $t(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_1x_3$, where the bit operations are the usual modulo 2 addition and multiplication.

   (a) (3p.) Create the values of the difference distribution table $N_D(a', b')$ of the function t, for $a' = 010$ and $a' = 111$ and all $b' \in \mathbb{Z}_2$.

   (b) (3p.) Show that t preserves complementation, that is, if each input bit is complemented then the output is complemented.

3. (6p.) Determine the three least significant decimal digits of the integer 2005^{2005}.

4. (6p.)

   (a) Evaluate the Jacobi symbol
   $$\left(\frac{801}{2005}\right).$$
   You should not do any factoring other than dividing out powers of 2.

   (b) Show that 2005 is an Euler pseudoprime to the base 801.

5. (6p.) Suppose that $n = 400271$ is the modulus and $b = 117353$ is the public exponent in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine also the secret exponent a and $\phi(n)$.