T-79.503 [old: T-110.503] Foundations of Cryptology
Exam
12.01.2004

1. (6 points) A 4-stage linear feedback shift register generates a sequence 1 0 1 0 0 0 1 0. Determine the feedback constants c_0, c_1, c_2 and c_3.

2. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$.

   a) (2 points) Create the look-up table for the function $f : z \mapsto z^3$ in $\mathbb{F}$.

   b) (2 points) Let $f_1(z)$ denote the rightmost bit of the output $f(z)$ of function f. Compute the algebraic normal form for f_1.

   c) (2 points) Show that the rightmost bit of the difference $f(z + 001) + f(z)$ is always equal to 1.

3. (6 points) It is given that

$$2^{48} \equiv 443 \pmod{1201},$$

   where 1201 is a prime. Show that the element $\alpha = 443$ is of order 25 in the multiplicative group $\mathbb{Z}_{1201}^*$.

4. (6 points) Using Shanks' algorithm attempt to determine x such that

$$443^x \equiv 489 \,(\mathrm{mod} 1201).$$

   Note that if this congruence has solutions, then according to problem 3 (see above) one solution is a positive integer less than 25.

5. (6 points) Alice is using the RSA Cryptosystem and her modulus is $n = 334501 = 167 \cdot 2003$. Decrypt the ciphertext $y = 2003$.