T-79.503 Foundations of Cryptology
Exam
December 10, 2004

1. (6 points) Let m be a positive integer. Consider a cryptosystem with $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^m$ and keys are chosen equiprobably. This cryptosystem is used to encrypt a language, which consists of strings of m-bit blocks that have exactly one non-zero bit. Each block is chosen independently and equiprobably. Estimate the unicity distance using the formula

$$n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|},$$

and show that the estimate is less than or equal to 2 for all m, except for $m = 3$.

2. (6 points) Let e_K be the encryption transformation of a block cipher with 64-bit key K and 64-bit block length. The key size of the block cipher is doubled as follows. Given two 64-bit keys K_1 and K_2 and a 64-bit plaintext x the ciphertext y is computed as

$$y = e_{K_2}(x \oplus K_1).$$

Assume that an attacker has two known plaintext-ciphertext pairs x_1, y_1 and x_2, y_2 encrypted in this manner with a 128-bit key (K_1, K_2). Show that then the attacker can do exhaustive search over a 64-bit partial key and find the entire key with a large success probability. Give an estimate of the success probability.

3. (6 points) Consider a finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^4 + x + 1)$, and a stream cipher with $\mathcal{P} = \mathcal{C} = \mathbb{F}$ and $\mathcal{K} = \mathbb{F}^* = \mathbb{F} - \{0\}$. This stream cipher is used to encrypt language, which consists of strings of 4-bit blocks that have exactly one non-zero bit. Given a key $K = \beta \in \mathbb{F}^*$ and a plaintext sequence $x_i,\ i = 1, 2, ...$, the keystream and the encryption rule are defined as follows

$$z_i = \beta^i, \text{ and } y_i = e_{z_i}(x_i) = z_i + x_i,\ i = 1, 2, ...$$

The 3rd term of the ciphertext sequence is

$$y_3 = 0111 = x^2 + x + 1.$$

Given this information, exactly three keys are possible. What are they?

4. (6 points) It is given that

$$12^{2004} \equiv 4815 \,(\mathrm{mod}\, 50101),$$

where 50101 is a prime. Show that the element $\alpha = 4815$ is of order 25 in the multiplicative group $\mathbb{Z}^*_{50101}$.

5. (6 points) Using Shanks' algorithm attempt to determine x such that

$$4815^x \equiv 48794 \,(\mathrm{mod}\, 50101).$$

Hint: See Problem 4.

Note: If you do not have a calculator, it suffices to explain what you would do if you had one.