T-79.503 Foundations of Cryptology
T-79.5501 Cryptology
Exam
October 24, 2005

1. (6 pts) A cryptosystem has a 128-bit key. The keys are generated as strings of octets. The generator is flawed, due to which each key octet has at most four non-zero bits. Each such octet has equal probability and the octets are independent. Compute the entropy of the key.

2. (6 pts) Consider the S-box S_4 of the DES:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

We restrict ourselves to inputs $(x_0, x_1, x_2, x_3, x_4, x_5)$ such that the output is taken from the fourth row. Recall that then some of the input bits are fixed. The output bits are approximated using the xor-sum $x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5$ of the input bits. The task is to determine the output bit for which this approximation works best.

3. (6 pts) 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 $\mathcal{K} = \mathbb{F}^* = \mathbb{F} - \{0\}$. 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

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

This stream cipher is used to encrypt a language, which consists of strings of 4-bit blocks that have exactly one non-zero bit. The 3rd term of the ciphertext sequence is $y_3 = \texttt{0011}$. Compute the key K. Is the solution unique?

4. (6 pts)

   (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. (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.