T-79.503 Foundations of Cryptology
Exam
May 11, 2004

1. (6 pts) Prove that, in any cryptosystem, $H(\mathbf{P}|\mathbf{C}) \leq H(\mathbf{K}|\mathbf{C})$. (Intuitively, this result says that, given a ciphertext, the opponent's uncertainty about the key is at least as great as his uncertainty about the plaintext.) You may use any results already proved in the textbook.

2. Assume that a sequence of plaintext blocks of length 128 bits have been encrypted using the AES block cipher in CBC mode.

   a) (3 pts) If two equal ciphertext blocks are detected, what can be said about the corresponding plaintext blocks?

   b) (3 pts) Estimate how many blocks need to be encrypted so that the probability of finding two equal ciphertext blocks becomes larger than 0.5?

3. (6 pts) Solve the following system of congruences

$$\begin{aligned} 15x &\equiv 12 \pmod{2003} \\ 11x &\equiv 5 \pmod{2004} \end{aligned}$$

4. (6 pts) Consider the Galois field $GF(2^3) = \mathbb{Z}_2[x]/f(x)$ where $f(x) = x^3 + x^2 + 1$. We define a mapping in it as $z \mapsto z^3$, for $z \in GF(2^3)$. This mapping defines a three-bit to three-bit S-box in a natural manner. Prove that this S-box is almost perfect nonlinear, that is, all entries in the difference distribution table $N_D(a', b')$ are either 0 or 2.

5. a) (3 pts) Describe the Solovay-Strassen primality test for an odd integer n, $n > 1$.

   b) (3 pts) Is $n = 115$ Euler pseudo-prime to the base $a = 6$?