T-79.503 [old: T-110.503] Foundations of Cryptology
Exam
03.09.2003

1. (6 points) Let us consider a Feistel cipher which has three rounds and is defined as follows. Denote the lenght of the data block by $2n$ and the plaintext by (L_0, R_0), where L_0 and R_0 each is a block of n bits. The following computations are performed:

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f_i(R_{i-1}), \end{aligned}$$

   where f_i is a function of n bits and $i = 1, 2, 3$. Ciphertext is (L_3, R_3). The Feistel cipher is a one-to-one mapping from the plaintext to the ciphertext, and for some particularly chosen functions f_1, f_2 and f_3, the three-round Feistel cipher is the identical mapping, that is, $L_0 = L_3$ and $R_0 = R_3$ for all plaintexts. Determine all such functions f_1, f_2 and f_3.

2. (6 points) Assume that AES block cipher is used in the CBC mode.

   a) Estimate the number of ciphertext blocks needed to have the probability of finding two equal ciphertext blocks to become larger than 0.5?

   b) Assume that two equal ciphertext blocks are detected, which have been produced using the same key (and the CBC mode). What can then be said about the corresponding plaintext blocks?

3. (6 points) Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables defined on the set $\{0, 1\}$. Let ϵ_i denote the bias of $\mathbf{X}_i$, $\epsilon_i = Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, for $i = 1, 2$. Prove that if the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent, then $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

4. (6 points) Solve the congruence equation

$$x^3 \equiv 9 \,(\mathrm{mod} 2003).$$

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