T-110.503 Basics of Cryptology
Exam
4.9.2002

1. (6 points) The key of a cryptographic system is 100 bits. Key generation is performed using a pseudorandom number generator which generates the key in blocks of five bits. The generator is flawed, due to which it produces five bit blocks where the number of ones is less than the number of zeroes. What is the effective key length of the keys produced by this generator, that is, how many bits of entropy the produced keys have?

2. (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). When this Feistel cipher is an identical mapping, that is, when $L_0 = L_3$ and $R_0 = R_3$ for all plaintexts?

3. (6 points) Let $n = pq$, where p and q are primes. We can assume that $p > q > 2$ and we denote $d = \frac{p-q}{2}$ and $x = \frac{p+q}{2}$. Then $n = x^2 - d^2$. Show that if $d < \sqrt{p+q}$ then x can be computed by taking the square root of n and by rounding the result up to the nearest integer.

   [If you have a pocket calculator available you can test this method to factorize $n = 4007923$.]

4. (6 points) The module is $2002 = 2 \times 7 \times 11 \times 13$. Solve one of the following problems. It is your choice, either a) or b).

   a) What is the number of solutions of the following congruence eaquation

   $$x^4 \equiv 9 \pmod{2002}$$

   b) What is the number of solutions of the following congruence equation

   $$x^9 \equiv 4 \pmod{2002}$$

5. (6 points) Describe how the keys for the RSA cryptosystem are created. Describe also how the enryption and decryption transformations are defined.