TIK-110.503 Foundations of Cryptology
Final exam
16.12.1999

1. (6 points) The DES block cipher is used as encryption transformation. The plaintext is comprised of four-bit blocks with exactly one 1-bit in each block.

   a) This plaintext is encrypted as such. Determine the unicity distance (in bits).

   b) Prior to encryption, randomly generated four-bit blocks are inserted in the plaintext after each four-bit block. Determine the unicity distance in this case.

2. (6 points) Consider a Feistel cipher, where the ith round is defined as follows:

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

   where K_i is the round key and F_i is the round function. Given a sequence A of bits we denote by $c(A)$ the sequence obtained by complementing the bits of A. For example, if $A = 001$ then $c(A) = 110$. Let $Y = (L_r, R_r)$ be the ciphertext obtained by encrypting the plaintext $X = (L_0, R_0)$ (= concatenation of L_0 and R_0) using the r-round Feistel cipher with round keys $K_1, K_2, \ldots, K_r$. The same Feistel cipher, with the same round functions, is used for encrypting $c(X)$. Show that there exist round keys such that the resulting ciphertext is equal to $c(Y)$.

3. a) (3 points) Prove that 12 is not a quadratic residue modulo 1999.

   b) (3 points) Prove that the congruence

$$16^x \equiv 12 (\mathrm{mod} 1999)$$

   does not have a solution.

4. (6 points) Bob and Bart are using the Rabin Cryptosystem. Bob's modulus is $n_1 = 2183$ and Bart's modulus is $n_2 = 2173$. Both have chosen $B = 0$. Alice has an integer x, $0 < x < 2173$, to be encrypted for both Bob and Bart. To Bob, she sends ciphertext $y_1 = 1111$ and to Bart, she sends $y_2 = 2027$. Determine x. (Ignore the fact that the prime factors of the moduli are not congruent to 3 (mod 4) as normally is the case in Rabin cryptosystem. You should find the solution without factoring the moduli.)

5. (6 points) Consider Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. Find the cyclic subgroups of $GF(2^4)^*$ which are strict subgroups, i.e., have less than 15 elements.