TIK-110.503 Foundations of Cryptology
Final exam
September 5, 2000

1. (6 points) The plaintext consists of blocks of five bits, where the number of ones is less than the number of zeros. Each such block occurs in the plaintext with equal probability. How many bits of redundancy does this plaintext contain per block?

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 bit sequence A we denote by $c(A)$ the bit 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 $K_1, K_2, \ldots, K_r$. Show that then the plaintext $c(X)$ encrypted using the round keys $c(K_1), c(K_2), \ldots, c(K_r)$ gives the ciphertext $c(Y)$.

3. (6 points) Solve the system of congruences

$$\begin{aligned} 3x + 7y &\equiv 0 (\mathrm{mod} 42) \\ 2x - 3y &\equiv 2 (\mathrm{mod} 42). \end{aligned}$$

4. (6 points) Number 59 is a square root of 1481 modulo 2000. Find some other square root of 1481 modulo 2000. Hint: Recall that if m_1 divides $a - b$ and m_2 divides $a + b$, and $\gcd(m_1, m_2) = 1$, then $a^2 \equiv b^2 \ (\mathrm{mod} m_1 m_2)$.

5. (6 points) Consider ElGamal Public-key Cryptosystem in Galois field GF(2^4) with polynomial $x^4 + x^3 + 1$ and with the primitive element $\alpha = 0010 = x$. Your private key is $a = 4$.

   a) Compute your public key β.

   b) Decrypt ciphertext (0100,1110) using your private key. Recall that given a plaintext X the ciphertext is $(\alpha^k, X\beta^k)$, where the integer k has been chosen by the encryptor and is not known to you.