TIK-110.503 Basics of Cryptology
Final exam
April 7, 2001

1. (6 points) Plaintext consists of equally likely strings of m bits with a single 1 bit. In each string the other $m-1$ bits are zeros.

   a) Determine the plaintext redundancy.

   b) This plaintext is encrypted using a cryptosystem with $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = 2^m$. Show that the unicity distance $n_0 \leq 2$, for all positive integers m except for $m = 3$. (Hint: $\log_2 3 \approx 1.585$.)

2. (6 points) Given a positive integer r and a combiner function $f : \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ we define a kind of *Feistel cipher* as follows:

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= (L_{i-1} + f(R_{i-1}, K_i)) \bmod 26, \end{aligned}$$

   where $K_i \in \mathbb{Z}_{26}$, and $i = 1, 2, \ldots, r$, and L_j, $R_j \in \mathbb{Z}_{26}$, $j = 0, 1, 2, \ldots, r$. The plaintext is (L_0, R_0) and the ciphertext is (L_r, R_r).

   Consider a case where $r = 2$, $K_1 = K_2 = K$, and the combiner function f is defined as $f(X, K) = (X \times K) \bmod 26$. The plaintext is (17,13) and the ciphertext is (4,13). Determine the key K.

3. (6 points) Let $n = pq$, where p and q are prime. We assume that $p > q > 2$ and denote the difference $p - q$ by d. Note that then d is positive and even.

   a) Let us assume that n and d are given. Show how then p and q can be computed.

   b) If n is given, and it is known that d is small, then one can try all possible values for d and compute the factors p and q. Use this method to factor 4003997.

4. (6 points) The modulus is $2001 = 3 \times 23 \times 29$. Does the congruence equation

$$x^4 \equiv 7 (\bmod 2001)$$

   have integer solutions for x?

5. (6 points) Consider ElGamal Public-key Cryptosystem in Galois field GF(2^4) with polynomial $x^4 + x + 1$ and with the primitive element $\alpha = 0010 = x$. Your private key is $a = 7$.

   a) Compute your public key β.

   b) Decrypt ciphertext (0100,1110) using your secret key. Recall that given a plaintext X the ciphertext is $(\alpha^k, X\beta^k)$, where the integer k is known only to the encryptor.