TIK-110.503 Basics of Cryptology
Final exam
September 4, 2001

1. (6 points) Consider a binary LFSR with connection polynomial $x^4 + x^3 + x^2 + x + 1$.
   a) Determine the periods of the binary sequences generated by this LFSR.
   b) Consider a stream cipher based on this LFSR. The ciphertext sequence is
   1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0
   and it is given that the fourth and twelth plaintext bits are equal to **0** and the eighth and sixteenth bits are equal to **1**. Find the initial state of the LFSR, that is, the four first bits of the keystream sequence.

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 $r = 2$, the key K is unknown, $K_1 = K$ and $K_2 = (K + 13) \bmod 26$, and the combiner function f is defined as $f(R_{i-1}, K_i) = (R_{i-1} \times K_i) \bmod 26$.

   a) Show that with a chosen plaintext (1,13) we have $R_2 = K$.
   b) Find a chosen plaintext, which gives $L_2 = K$.

3. a) (3 points) Give the Solovay-Strassen primality test for an odd integer n, $n > 1$.
   b) (3 points) Is 21 Euler pseudo-prime to the base 2?

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

$$x^4 \equiv 9 \pmod{2001}$$

   have integer solutions for x?

5. (6 points) Consider a variation of El Gamal Signature Scheme in $GF(2^n)$. The public parameters are n, q and α, where q is a divisor of $2^n - 1$ and α is an element of $GF(2^n)$ of multiplicative order q. A user's secret key is $a \in \mathbb{Z}_q$ and the public key β is computed as $\beta = \alpha^a$. To generate a signature for message x a user with secret key a generates a secret value $k \in \mathbb{Z}_q^*$ and computes the signature (γ, δ) as

$$\begin{aligned} \gamma &= \alpha^k \text{ (in } GF(2^n)) \\ \delta &= (x - a\gamma')k^{-1} \bmod q, \end{aligned}$$

   where γ' is an integer representation of γ. Suppose Bob is using this signature scheme, and he signs two messages x_1 and x_2, and gets signatures (γ_1, δ_1) and (γ_2, δ_2), respectively. Alice sees the messages and their respective signatures, and she observes that $\gamma_1 = \gamma_2$.

   a) Describe how Alice can now derive information about Bob's private key.
   b) Suppose $n = 8$, $q = 15$, $x_1 = 1$, $x_2 = 4$, $\delta_1 = 11$, $\delta_2 = 2$, and $\gamma'_1 = \gamma'_2 = 7$. What Alice can say about Bob's private key?