TIK-110.503 Basics of Cryptology
Final exam
January 12, 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) The DES keys are 64 bits sequences, where each eighth bit is a parity bit computed as a modulo 2 sum of the preceding seven bits. A key management center uses DES encryption algorithm and a "master" DES key to encrypt DES keys to end users. Each ciphertext block consists of one encrypted DES key. Estimate the unicity distance of this cryptosystem, that is, the average number of encrypted end users' DES keys needed to uniquely compute the master key given enough computing time.

3. (6 points) The T function used in the hash-function SHA-1 is defined as follows. Let X_0, X_1, X_2 be three 32-bit blocks. Then $T(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$, where $\wedge$ is bitwise "and" multiplication, and $\vee$ is bitwise "or" addition. Let $t(x_0, x_1, x_2)$ denote the Boolean function of three variables which is the one-bit component of T.

   a) Determine the algebraic normal form of the Boolean function t.

   b) A *linear structure* of a Boolean function f of three variables is defined as a vector $w = (w_1, w_2, w_3) \neq (0, 0, 0)$ such that $f(x \oplus w) \oplus f(x)$ is constant. Show that t has exactly one linear structure.

4. (6 points) Prove that the congruence

   $$x^{12} \equiv x^1 (\mathrm{mod}\, 2001)$$

   has solutions $x \neq 0$ or 1. (Hint: $2001 = 3 \times 23 \times 29$.)

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?