T-110.503 Basics of Cryptology
Exam
08.01.2003

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 where the keystream is generated as output of this LFSR. The first 19 bits of the ciphertext sequence are

      `1 1 1 1 1 1 0 1 0 0 0 0 0 0 1 1 1 0 1`

      and it is given that the 16th, 17th, 18th and 19th plaintext bits are

      `0 1 0 0.`

      Find the initial state of the LFSR, that is, the first four bits of the keystream sequence.

2. (6 points) Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables defined on the set $\{0,1\}$. Let ϵ_i denote the bias of $\mathbf{X}_i$, for $i=1,2$. Prove that if the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent, then $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

3. (6 points) A prime p is said to be a *safe prime* if $(p-1)/2$ is a prime.

   a) Let p be a safe prime, that is, $p = 2q+1$ where q is a prime. Prove that an element in $\mathbb{Z}_p$ has multiplicative order q if and only if it is a quadratic residue and not equal to 1 mod p.

   b) The integer 08012003 (which represents the date of this exam) is a safe prime, since 4006001 is a prime. Generate an element of multiplicative order 4006001 in $\mathbb{Z}_{8012003}$.

4. (6 points) It is given that

$$2^{120} \equiv 15068 (\mathrm{mod} 122183).$$

   Using the $p-1$ method, attempt to factor 122183.

5. (6 points) Consider the *ElGamal Public-key Cryptosystem* in the finite field $\mathbb{Z}_2[x]/(x^3+x+1)$. The private key is $a=3$ and the primitive element is $\alpha = \mathtt{010}$. Compute the public key β, and decrypt the ciphertext $(\mathtt{110}, \mathtt{110})$.