T-110.503 Basics of Cryptology
Exam
9.5.2003

1. Consider a binary LFSR with connection polynomial $x^4 + x^3 + x^2 + x + 1$.

   a) (3 points) Show that the periods of the binary sequences generated by this LFSR are 1 and 5.

   b) (3 points) Consider a stream cipher where the keystream is generated as output of this LFSR. The first 19 bits of the ciphertext sequence are

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

      and it is given that the 16th, 17th, 18th and 19th plaintext bits are `0 0 0 0`. Decrypt the ciphertext.

2. Consider a cryptosystem where $\mathcal{P} = \{A, B\}$ and $\mathcal{C} = \{a, b, c\}$, $\mathcal{K} = \{1, 2, 3, 4\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(A)$	$e_K(B)$
1	a	b
2	b	c
3	b	a
4	c	a

   The keys are chosen with equal probability.

   a) (3 points) Show that

   $$\mathbf{Pr}[\mathbf{x} = A | \mathbf{y} = b] = \frac{2\mathbf{Pr}[\mathbf{x} = A]}{1 + \mathbf{Pr}[\mathbf{x} = A]}.$$

   b) (3 points) Does this cryptosystem have perfect secrecy?

3. Consider a finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3+x+1)$. Let an S-box with three input bits and three output bits be defined using the function $\pi_S(w) = w^3$, for $w \in \mathbb{F}$. For example, if $w = \texttt{011} = x+1$ then $\pi_S(w) = \pi_S(x+1) = (x+1)^3 = x^3+x^2+x+1 = x^2 = \texttt{100}$.

   a) (3 points) Let $a' = \texttt{100} = x^2$. Show that

   $$\pi_S(w + a') + \pi(w) = x^2w^2 + (x^2 + x)w + x^2 + 1, \text{ for all } w \in \mathbb{F}.$$

   b) (3 points) Compute the row of the *Difference Distribution Table* of π_S corresponding to the input difference $a' = \texttt{100}$. Note that you can use the result of item a).

4. (6 points) Consider $p = 2003$, which is a prime. Find an element of order $q = 11$ in the multiplicative group $\mathbb{Z}^*_{2003}$.

5. (6 points) Suppose that $n = 355044523$ is the modulus and $b = 311711321$ is the public exponent in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n.