T-79.5501 Cryptology
Homework 3
October 6&7, 2005

1. Determine the two least significant decimal digits of the integer 2005^{2005}.

2. (Stinson 5.9) Suppose that $p = 2q + 1$, where p and q are odd primes. Suppose further that $\alpha \in \mathbb{Z}_p^*$, $\alpha \neq \pm 1 (\mathrm{mod} p)$. Prove that α is a primitive element modulo p if and only if $\alpha^q \equiv -1 \, (\mathrm{mod} p)$.

3. Find the smallest primitive element in $\mathbb{Z}_{17}^*$. (Hint: use the result of problem 2.) What are the orders of elements 2 and 4? Give 2 and 4 as powers of the smallest primitive element.

4. Consider the Galois field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))$, with the polynomial $f(x) = x^5 + x^2 + 1$. Perform the following computations in this field.

   a) Compute $(x^4 + x)(x^3 + x^2 + 1)$.
   b) Using the Euclidean Algorithm, compute $(x^3 + x)^{-1}$.
   c) Compute x^{35}. (Hint: $x^5 = x^2 + 1$.)

5. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))$, where $f(x) = x^4 + x + 1$. Plaintext consists of equally likely strings of 4 bits with a single 1 bit. In each string the other 3 bits are zeros. The encryption method is a stream cipher with $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{F}^*$. Given a key $K = \beta \in \mathbb{F}^*$ and a plaintext sequence x_i, $i = 1, 2, \ldots$, the keystream and the encryption rule is defined as follows

   $$z_i = \beta^i, \text{ and } y_i = e_{z_i}(x_i) = \beta^i x_i, \; i = 1, 2, \ldots.$$

   It is given that the 3rd and 4th terms of the ciphertext sequence are

   $$y_3 = 1100 \text{ and } y_4 = 0111.$$

   Then exactly two keys are possible. What are they? (Hint: To facilitate the computations you may represent the elements of $\mathbb{F}^*$ as powers of a primitive element α. For example, if you choose $\alpha = 0010$, then the four possible plaintext terms are 1, α, α^2 or α^3.)

6. Consider Galois field $\mathbb{F} = \mathbb{Z}[x]/(m(x))$ with polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. The elements of $\mathbb{F}$ are given as octets `XY` using hexadecimal notation. Suppose that two polynomials $c(x)$ and $d(x)$ with coefficients in $\mathbb{F}$ are given as follows:

   $$\begin{aligned} c(x) &= \mathtt{03}x^3 + \mathtt{01}x^2 + \mathtt{01}x + \mathtt{02} \\ d(x) &= \mathtt{0B}x^3 + \mathtt{0D}x^2 + \mathtt{09}x + \mathtt{0E} \end{aligned}$$

   Show that $c(x)d(x) = \mathtt{01}(\mathrm{mod}\ (x^4 + \mathtt{01}))$. The polynomial $c(x)$ defines the MixColumn transformation in Rijndael and $d(x)$ defines its inverse transformation.

7. (Stinson 6.4 (a)) Suppose that p is an odd prime and k is a positive integer. The multiplicative group $\mathbb{Z}_{p^k}^*$ has order $\phi(p^k) = p^{k-1}(p-1)$, and is known to be cyclic. A generator of this group is called a *primitive element modulo* p^k. Suppose that α is a primitive element modulo p. Prove that at least one of α or $\alpha + p$ is a primitive element modulo p^2.