MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #8

Problems for all

Problem 1. Find all monic irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$.

Problem 2. Verify that the Rijndael polynomial

$$f(X) = X^8 + X^4 + X^3 + X + 1$$

is irreducible in $\mathbb{F}_2[X]$. *[Hint: If it has a factor, it must have degree at most* 4.*]*

Problem 3. Put $f(X) = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$, and let

$$a = 00001100 = X^3 + X^2 \in F = \mathbb{F}_2[X]/(f).$$

(a) Compute a^5.
(b) Find the inverse $f^{-1} \in F$ of $f = X^2 = 00000100$.
(c) Multiply $f^{-1}a$ and verify that $f^{-1}a = X + 1$ in F.

Additional problems for 395A

Problem 4. Let p be prime and define

$$a_n(p) = \#\{f \in \mathbb{F}_p[X] : \deg f = n,\ f \text{ monic irreducible}\}.$$

(a) Show that $a_2(p) = (p^2 - p)/2$ and $a_3(p) = (p^3 - p)/3$.
(b) Use the equality

$$(*) \qquad \sum_{d|n} d a_d(p) = p^n$$

(which you may assume) to compute $a_2(n)$ for $n = 1, \ldots, 10$.
(c) Use $(*)$ to prove that

$$\frac{p^n - 2p^{n/2}}{n} < a_n(p) \leq \frac{p^n}{n}.$$

Conclude that the probability that a random monic polynomial of degree n over $\mathbb{F}_p$ is irreducible is roughly $1/n$.

Problem 5. Let k be a finite field, $\#k = q$, and let $k[X]$ be the ring of polynomials with coefficients in k. For $f = \sum_{i=0}^{n} c_i X^i \in k[X]$ and $a \in k$, write $f(a)$ for the element $\sum_{i=0}^{n} c_i a^i$ of k.

(a) Let $b \in k$ and define $f = 1 - (X - b)^{q-1}$. Prove:

$$f(a) = \begin{cases} 0, & a \in k,\ a \neq b; \\ 1, & a = b. \end{cases}$$

Date: Due Wednesday, 29 October 2008.

(b) Prove that there are precisely q^q different maps $g : k \to k$ and that for each of them there is a unique polynomial $f \in k[X]$ of degree $< q$ such that for all $a \in k$ one has $g(a) = f(a)$. (In other words, *every* map between finite fields is given by a polynomial map.)

Computational challenges

Problem C2. Write a computer program that performs one round of AES with a key size of 128 bits.