Cryptography I, homework sheet 7

Due: 25 November 2011, 10:45

The Rabin irreducibility test is given as a lemma below. More details on finite fields and a proof of the lemma can be found in Tanja's script on finite fields posted on the webpage.

1. Let $q = p^n$ be a prime power and let $\mathbb{F}_q$ be a finite field with q elements. Show that $x^q - x$ has only simple roots and that

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

   Hint: You can use exercise 5 from sheet 6.

2. Use the Rabin test to prove that $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. You should be able to do this exercise by hand. Please document the results of all steps in the algorithm and show how they were obtained.

3. Use the Rabin test to prove that $x^{121} + x^2 + 1$ is not irreducible over $\mathbb{F}_2$. For this exercise you should use a computer algebra system. Please document the results of all steps in the algorithm and show how they were obtained; show how you worked around needing to work with polynomials of degree 2^{121}.

Lemma 1 (Rabin test)
The polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $\deg(f) = m$ is irreducible if and only if

$$f(x) | x^{q^m} - x$$

and for all primes $d < m$ dividing m one has

$$\gcd(f(x), x^{q^d} - x) = 1.$$