Cryptography I, homework sheet 7

Due: 19 November 2010, 10:45

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 3 from sheet 6.

2. Count the number of irreducible polynomials of degree 30 over $\mathbb{F}_3$.

3. Use the Miller Rabin test to prove that $x^4 + x + 1$ is 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.

4. Use the Miller 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 and how you worked around needing to work with polynomials of degree 2^{121}.