Cryptography I, homework sheet 6

Due: 17 October 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.

Please email Tanja in case you have found no way of obtaining a programmable calculator to use for the exam.

1. Consider the residue classes of $\mathbb{F}_2[x]$ modulo $f(x) = x^n + 1$ for some positive integer $n > 1$, i.e. $R = \mathbb{F}_2[x]/(x^n + 1)$. Note that R can be represented as

$$R = \left\{ a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_2 \right\}.$$

   Show that R is not a field, i.e. find a non-zero element that is not invertible or that gives 0 when mulitplied with another non-zero element.

2. Let K be a field of characteristic p, where p is prime. Show that for any integer $n \geq 0$ one has

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

   for all $a, b \in K$.
   Hint: You can use the binomial theorem and use proof by induction.

3. Compute $N_3(4)$, the number of irreducible polynomials of degree 4 over $\mathbb{F}_3$.

4. 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}.