Institut for Matematik og Datalogi
Syddansk Universitet

October 30, 2006
JFB

Cryptology – E06 – Week 8

Lecture, October 26

We finished chapters 5 and 6. on chapter 6.

Lecture, November 2

We will cover the McEliece Cryptosystem (copied from an earlier edition of the textbook), introduce digital signatures from chapter 7, and begin on chapter 4.

Lecture, November 9

We will finish chapter 4, skipping section 4.3.1. We will continue in chapter 7.

Problem session November 6

1. Do problems 6.12, 6.16a, 6.20 (work in the multiplicative group modulo 1103), and 6.22 in the textbook.

2. In class we have discussed the discrete logarithm problem modulo a prime, which means that we have discussed them over fields of prime order. There are also finite fields of prime power order, so for any prime p and any exponent $e \geq 1$, there is a field with $q = p^e$ elements, $GF(q)$. The elements of such a field can be represented by polynomials over $GF(p)$ of degree no more than $e-1$. The operations can be performed by working modulo an irreducible polynomial of degree e. For example, $y = x + x^5 + x^7$ is an element of the field $GF(2^{10})$, represented by $GF(2)[x]/(x^{10} + x^3 + 1)$. One can calculate a representation for y^2, by squaring y and then computing the result modulo $x^{10} + x^3 + 1$,

so one gets $x^2 + 2x^6 + 2x^8 + x^{10} + 2x^{12} + x^{14} \pmod{x^{10} + x^3 + 1} = 1 + x^2 + x^3 + x^4 + x^7$. In Maple, you can use the `powmod` function to do these calculations.

Try raising y to the powers $e \in \{33, 93, 341, 1023\}$ to see what result you get. What do you get? What does this prove about y?

3. On my computer using Mathematica (last time I tried), raising to the power 1023 directly failed due to lack of memory. What does this say about how Mathematica did the calculations? What can you do to get around this problem when you try these calculations? (Maple has no problems with these calculations.)

4. Why would there be a preference for working in $GF(2^k)$ for some large k, rather than modulo a prime for some very large prime? Hint: think about how arithmetic is performed.