Institut for Matematik og Datalogi — March 4, 2008
Syddansk Universitet — JFB

Cryptology – F08 – Week 7

Lecture, February 28

We continued with chapter 5.

Lecture, March 3

We finished chapter 5.

Lecture, March 7

We will begin on chapter 6 and possibly cover the McEliece Cryptosystem (copied from the earlier edition of the textbook).

Lecture, March 13

We will cover the McEliece Cryptosystem, begin on digital signatures from chapter 7, and start on chapter 4.

Problem sessions March 10 and 14

1. Do problem 5.26. It is easy to program with Maple. You will probably use a loop including something like `while (igcd(x2-x1,262063)=1) do ... end do;`.
2. Do problem 5.27. Note that it is sufficient to start with 507, skip everything between 517 and 528, and continue to 531, so you can do this interactively in Maple.
3. Do problem 5.28a.

4. Do problem 5.29. Note that for part c, $d = 9$ works.

5. Do problem 5.34.

6. Assume that $p \equiv q \equiv 3 \pmod 4$ and $n = pq$. Assume that r is chosen at random from the uniform distribution over Z_n^*. Show that $r^2 \pmod n$ is a random quadratic residue modulo n from the uniform distribution. Show that $-r^2 \pmod n$ is a random quadratic nonresidue with Jacobi symbol $+1$, also from the uniform distribution over these values.

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

8. 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?

9. 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.)

10. 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.

11. Do problem 4.1 in the textbook. For part (d), use the fact that the left-hand side in (c) is at least zero.

12. Do problem 4.6.