Institut for Matematik og Datalogi
Syddansk Universitet

March 6, 2013
JFB

Cryptology – F13 – Week 6

Lecture, March 4

We covered chapter 6 in the textbook, plus section 10.2 on Diffie-Hellman key distribution.

Lecture, March 8

We will cover the McEliece Cryptosystem (copied from the earlier edition of the textbook and sent to you via e-mail). You can look at Regev's articles in STOC '05 and CRYPTO 06 for another system secure against quantum attacks, and at Peikert's papers on lattice-based systems: http://eprint.iacr.org. Then we will introduce digital signatures from chapter 7, and start on chapter 4, probably covering through section 4.2. A meet-in-the middle attack will be demonstrated.

Lecture, March 14

We will finish chapter 4, skipping the subsection on the Merkle–Damgård construction. We will also cover SHA-3, Keccak. See the course homepage for Keccak's specification.

Problem session March 11

1. Do problems 5.14, 5.18, 5.22, and 5.25 in the textbook.

2. Suppose you, as a cryptanalyst were interested in an RSA modulus N, and you were given a t such that $a^t \equiv 1 \pmod{N}$ for all $a \in Z_N^*$. (Note that t is not necessarily $\phi(N)$. In the case $N = 69841$, $\phi(69841) = 69300$, but t could have many other values including 2310 and 138600.)

a Give an efficient algorithm for determining the message m which was encrypted using the public exponent e, producing the cryptotext c.

b Give an efficient algorithm for factoring N. (Hint: some ideas from the Miller-Rabin primality testing algorithm may be helpful.)

3. I may lecture at the end.

Problem session March 15

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

7. 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?

8. 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.)

9. 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.

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

11. Do problem 4.6.

12. I may lecture at the end.