Institut for Matematik og Datalogi
Syddansk Universitet

March 7, 2011
JFB

Cryptology – F11 – Week 6

Lecture, March 1

We finished chapter 5.

Lecture, March 4

We will begin on chapter 6. and cover the McEliece Cryptosystem

Lecture, March 9

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

Problem session March 10

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.)

Assignment due Friday, March 18, 15:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three.

1. The Rabin Cryptosystem has the disadvantage that the encryption function $e_K(x) = x^2 \pmod{n}$ is not an injection, so decryption is not necessarily unique. Consider the following restriction where $p = 2p'+1$, $q = 2q' + 1$, and p, p', q, q' are all primes. Restrict messages to be encrypted to be values between 1 and $\min\{p', q'\}$. Now use the same encryption function as for the Rabin Cryptosystem.

   a. Is this encryption function an injection (1-1)? Why or why not?

   b. Is this cryptosystem secure? Why or why not?

2. Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume $(n = pq, e)$ is the public key. Suppose also that someone tells us they know one of the plaintext blocks has a common factor with n.

   a. Does this help us find the plaintext used to produce these blocks? If so, how? If not, why not?

   b. Can one use CBC mode (cipher block chaining mode) with RSA? Can one use OFB mode (outputfeedback mode) with RSA?

   c. For both CBC and OFB mode, how would using these modes this affect your answer to part (a)? Why?

3. Suppose that $n = pq$ is odd, and p and q are prime. Suppose that 5 divides $(q - 1)$, but not $(p - 1)$.

   a. How many fifth roots of 1 are there, i.e. how many x are there such that $x^5 \equiv 1 \pmod{n}$? Why?

   b. Suppose you had a probabilistic polynomial time algorithm for finding a fifth root of an arbitrary value x in Z_n^* (assuming x had a fifth root), i.e. y such that $y^5 \equiv x \pmod{n}$. How would you use this algorithm to factor n?

   c. Suppose your algorithm found fifteenth roots instead. Could you also use this? If so, how?

4. Consider a composite number N, which is the product of two primes. Suppose you are given a quadratic nonresidue, y, modulo N, such that the Jacobi symbol $\left(\frac{y}{N}\right) = 1$. Consider the following algorithm: Randomly choose $x \in Z_n^*$ and compute $z \leftarrow x^2 \cdot y \pmod{N}$.

   a. Prove that z is a random quadratic nonresidue modulo N with Jacobi symbol $+1$.

   b. Suppose that $\left(\frac{y}{N}\right) = -1$. What can you say about the result of the same algorithm? Why?