Institut for Matematik og Datalogi
Syddansk Universitet

October 6, 2006
JFB

Cryptology – E06 – Week 6

Lecture, October 5

We continued with chapter 5, covering the Jacobi symbol, a Monte Carlo algorithm for finding square roots modulo a prime, and the Miller-Rabin primality test. We also began studying the security of RSA.

Lecture, October 12

We will finish chapter 5 and possibly begin on chapter 6.

Lecture, October 26

We will continue with chapter 6 and cover the McEliece Cryptosystem (copied from the earlier edition of the textbook).

Problem session October 23

1. Do problems 5.14, 5.18, 5.22, and 5.25 in the textbook.
2. Compute the Jacobi symbols $\left(\frac{39}{73}\right)$, $\left(\frac{25}{77}\right)$, and $\left(\frac{29}{83}\right)$.
3. 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 $a \in \mathbb{Z}_N^*$. (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.)