Institut for Matematik og Datalogi
Syddansk Universitet

March 17, 2005
JFB

Cryptology – F05 – Lecture 7

Lecture, March 11

We continued with chapter 5, covering Legendre and Jacobi symbols and finding square roots modulo primes and composites.

Lecture, March 18

We will continue with chapter 5.

Lecture, April 1

We will finish chapter 5 and begin on chapter 6.

Problem session March 30

We will finish chapter 5 and

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.)