Institut for Matematik og Datalogi
Syddansk Universitet

April 14, 2005
JFB

Cryptology – F05 – Lecture 10

Lecture, April 8

We covered the McEliece Cryptosystem (copied from the earlier edition of the textbook), introduce digital signatures from chapter 7, and began on chapter 4, covering up through the introduction to SHA-1.

Lecture, April 15

We will finish chapter 4, skipping section 4.3.1. We will continue in chapter 7.

Lecture, April 29

We will finish chapter 7, skipping sections 7.5 and 7.7. The description of undeniable signatures will follow that handout given in class.

Problem session April 20

Bring your second assignment. We will use time at the end to go over the last problem from that assignment.

1. In the discussion of the Schnorr signature scheme on page 286, it says that to find a qth root of 1 modulo p, one should begin with a primitive element α_0 of Z_p and compute $\alpha_0^{(p-1)/q}$.

   a. Why is this correct? What subgroup does the result generate?

   b. How long does it take to do this computation?

   c. Is it necessary that α_0 be a primitive element?

2. Suppose $p \equiv q \equiv 3 \pmod 4$ are both primes and $n = p \cdot q$. Suppose x is a QNR modulo both p and q. Show that $-x$ is a QR modulo n.

3. Do problem 6.21 in the textbook.

4. Do problem 7.1 in the textbook. (You might want to look at the notes on the course home page on number theory to recall how to solve linear congruences.)

5. In the Diffie-Hellman key-exchange system (Figure 8.2) from the handout, consider the possibility that the number α is not a generator.

   a. Would a pair of users still be able to agree on a key?

   b. When the two users agree on a key, what effect would the fact that α is not a generator have on an eavesdropper's ability to determine that key?