Institut for Matematik og Datalogi
April 14, 2003

Institut for Matematik og Datalogi
Syddansk Universitet

April 14, 2003
JFB

Cryptology – F03 – Note 10

Lecture, April 8

We covered hash functions from chapter 4, skipping section 4.3.1.

Lecture, April 15

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

Lecture, April 29

We will finish chapter 7, and begin on protocols. There are handouts for this; it is not in the textbook.

Problems for Thursday, May 1

1. Do problem 47.6 in the textbook.
2. 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?
3. In the verification protocol for undeniable signatures (in the textbook), the verifier chooses randomly two values e_1 and e_2. Why are there two values? Why not just let $e_2 = 0$ always?

4. 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.

5. In the Diffie-Hellman key-exchange system (Figure 8.5), 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 g is not a generator have on an eavesdropper's ability to determine that key?