Institut for Matematik og Datalogi
Syddansk Universitet

April 6, 2005
JFB

Cryptology – F05 – Lecture 9

Lecture, April 1

We covered chapter 6 and Diffie-Hellman key exchange from some notes (copied from the earlier edition of the textbook). We began on the McEliece Cryptosystem.

Lecture, April 8

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

Lecture, April 15

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

Problem session April 13

Bring your second assignment. We will use time at the end to go over some of the problems from that assignment.

1. Do problem 4.1 in the textbook, but for part (c), the right-hand side of the inequality is wrong. It should be $\sum_{y \in Y}(s_y - \overline{s})^2 \leq 2S + N - \frac{N^2}{M}$. For part (d), use the fact that the left-hand side in (c) is at least zero.

2. Do problem 4.6.

3. Do problem 4.12. For part (b), you can find a (1,1)-forger. Skip the difficult case mentioned.

4. Let p be an odd prime and g_0 and g_1 be generators of $\mathbb{Z}_p^*$. Consider the following two functions: $f_0(x) = g_0^x \pmod{p}$ and $f_1(x) = g_1^x \pmod{p}$. Use these two functions which to create a hash function which will hash an arbitrary length message down to a value in $\mathbb{Z}_p^*$. Can you make it secure under the assumption that the discrete log problem is infeasible?