Institut for Matematik og Datalogi
Syddansk Universitet

April 7, 2003
JFB

Cryptology – F03 – Note 9

Lecture, March 25

We covered the first four sections of chapter 6, introduced digital signature schemes from chapter 7, and motivated the study of hash functions from this.

Lecture, April 8

We will begin on hash functions from chapter 4, skipping section 4.3.1.

Lecture, April 15

We will continue with chapter 7.

Problems for Thursday, April 24

1. Do problem 4.1 in the textbook, but for part (c), the right-hand side of the inequality is wrong. I should be $2S + N - \frac{N^2}{M}$. 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?