Institut for Matematik og Datalogi
Syddansk Universitet

April 14, 2008
JFB

Cryptology – F08 – Week 10

Lecture, April 8

We covered SHA–1, SHA–256, and the last two sections of chapter 4. Then we returned to chapter 7, covering up through section 7.4.2.

Lecture, April 10

We discussed subliminal channels and began on chapter 8, covering up through section 8.2 and section 8.4.

Lecture, April 16

We will cover section 8.3 and 7.6 (actually from some notes) and begin on zero-knowledge (from the notes by Ivan Damgård and Jesper Buus Nielsen, available through the course's homepage).

Discussion section April 17

At 8:30, this one time.

Lectures, April 22 and 24

We will continue with zero-knowledge, from the notes and slides, and begin on chapter 9 in the textbook.

Problem session April 23

1. Do problem 8.7. Use the following definition of period: $z_{i+t} = z_i$ for all $i \geq c$ for some c (i.e. it should be ultimately periodic). (The result

holds with the original definition, though.) For part b, use p=7 and q=11. Try with seed 4. Why can't you start with seed 2? :-)

2. Do exercises 1 through 7 in the notes by Damgård and Nielsen.