Institut for Matematik og Datalogi
Syddansk Universitet

May 17, 2011
JFB

Cryptology – F11 – Week 14

Lecture, May 16

We covered section 10.5.4 of chapter 10, section 11.2 of chapter 11, and section 13.1 of chapter 13. Then we began on quantum cryptography.

Lecture, May 19, from 11:15 to 12

We will finish quantum cryptography from Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography", J. of Cryptology 5, 1992. This can be found on-line through SDU's library (under the archived volumes of that journal). Then we will begin on quantum computing from R. de Wolf's survey on Quantum computation and Shor's factoring algorithm, which can be accessed through the course's homepage.

Lecture, May 25

We will finish quantum computing. We may also cover up through section 13.2.1 in chapter 13 and up through Theorem 10.4 in section 10.4 in the textbook.

Problem session May 23

1. Continue with any unfinished problems from last week.
2. What group would you use for Diffie-Hellman Key Predistribution?
3. How might you remove the possibility of a Man-in-the-Middle attack in the Diffie-Hellman Key Agreement Scheme?
4. Do problem 10.1 d.

5. Do problem 10.7.

6. Do problem 10.8.

7. Let x, y be two bit strings of length n. Suppose $x \neq y$. Choose a random subset S of the n indices and let $x' = \sum_{s \in S} x_s \pmod 2$ and $y' = \sum_{s \in S} y_s \pmod 2$. Prove that the probability that $x' \neq y'$ is exactly $1/2$.

8. Explain why removing the last bit from a set removes any information given by the parity of that set.