Institut for Matematik og Datalogi
Syddansk Universitet

May 10, 2013
JFB

Cryptology – F13 – Week 12

Lecture, May 10

We finished chapter 9 in the textbook and covered chapter 10. We skipped sections 10.3 through 10.5.3. We covered Shamir's secret sharing scheme from section 13.1 of chapter 13.

Lecture, May 16

We will finish section 13.1 of chapter 13 in the textbook and begin on 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).

Problem sessions May 13 and 17

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. Consider the Shamir secret sharing with $p = 31$. Let the threshold be $t = 3$. Suppose the shares are:

- (1, f(1)) = (1,16)
- (2, f(2)) = (2,5)
- (3, f(3)) = (3,5)

which are distributed to the share recipients. Show how to compute the secret.

8. I may lecture at the end on May 13.

9. 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.

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

11. I may lecture at the end on May 17.