Institut for Matematik og Datalogi
Syddansk Universitet

February 4, 2008
JFB

Cryptology – F08 – Week 3

Lecture, February 4

We finished chapter 1 in the textbook, skipping the Hill Cipher and covered sections 2.1, 2.4, 2.5 and 2.6 of chapter 2.

Lecture, February 8

We will cover sections 2.2, 2.3, and 2.7 of chapter 2 and 3.5, 3.5 and 3.7 of chapter 3 in the textbook (we will skip most of the first four sections). The original Rijndael specification (which can be found through the course's homepage) will be used as the basis for the description of AES.

Lecture, February 14

We will begin on chapter 5 in the textbook. My plan is to skip section 5.2.1 on the Extended Euclidean Algorithm. Please let me know if you haven't seen it before.

No class February 15

Problem session February 11

1. Problem 2.4 in the textbook.
2. Problem 2.10 in the textbook.
3. Problem 2.11 in the textbook.
4. Problem 2.17 in the textbook.

5. Suppose a cryptosystem has $P = \{a, b, c\}$, $C = \{1, 2, 3, 4\}$ and $K = \{K_1, K_2, K_3\}$. The encryption rules are as follows:

	a	b	c
K_1	1	2	3
K_2	4	3	2
K_3	3	4	1

   Suppose $p_K(K_i) = 1/3$ for $1 \leq i \leq 3$, $p_P(a) = 1/2$, $p_P(b) = 1/3$, and $p_P(c) = 1/6$.

   a. Compute the probabilities $p_C(y)$ for all $y \in \{1, 2, 3, 4\}$.

   b. Does this cryptosystem achieve perfect secrecy? Explain your answer.

6. Do problem 3.3 in the textbook.

7. Do problem 3.7 in the textbook.