Institut for Matematik og Datalogi
Syddansk Universitet

February 17, 2003
JFB

# Cryptology – F03 – Note 3

## Textbook

## Lecture, February 11

We finished chapter 1 in the textbook, skipping the Hill Cipher and began on chapter 2, covering section 2.1 and the first part of section 2.4.

## Problem session February 13

After discussing the problems, we covered the Extended Euclidean Algorithm (notes from DM11) and the Chinese Remainder Theorem (section 5.2.2 in the textbook). Slides from these and the lectures on algebra can be found on the course's homepage.

## Lecture, February 18

We will finish chapter 2 in the textbook.

## Lecture, February 25

We will begin on chapter 3 in the textbook.

## Problems for Thursday, February 27

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.