Institut for Matematik og Datalogi
Syddansk Universitet

January 26, 2008
JFB

Cryptology – F08 – Lecture 1

Textbook

Douglas R. Stinson, *Cryptography: Theory and Practice*, Third Edition, Chapman and Hall/CRC, 2006. There will also be supplementary notes.

Format

The course will be taught by Joan Boyar. The lectures will be in English. The course will be at 8:15 on Mondays, and 12:15 on Thursdays and Fridays, in the seminar room. The first two classes will be lectures, but after that we will alternate between lectures and discussion sections. Class is cancelled on February 15 and February 21.

There will be assignments which must be approved in order to take the written exam in January. The assignments are considered "exam projects". Thus, you may not work with anyone not in your group. The assignments must be turned in on time. There will be a chance to redo at most two assignment (of the four or five), if it is either late or not good enough the first time.

The weekly notes and other information about the course are available through the WorldWideWeb. Use the URL:

http://www.imada.sdu.dk/~joan/crypt/index.html.

My office hours will be Mondays from 10:30 to 11:15 and Thursdays from 9:00 to 9:45.

Lecture, January 28

We will begin with an introduction to the course. Then, we will cover sections 1.1.1–1.1.4 and 1.2.1–1.2.3 in the textbook. We may also cover the Vigenere cipher if there is time.

Lecture, January 31

We will cover the discrete math notes on algebra (starting on page 6 of the notes or 181 of the slides) from the home page for the course, plus those on the Extended Euclidean Algorithm (section 5.2.1 in the textbook).

Lecture, February 4

We will continue with chapter 1 in the textbook, skipping the Hill Cipher and begin on chapter 2. We will skip Huffman coding, which is covered in DM507.

Problem session February 1

1. This was encrypted using a Caesar cipher. Decipher it.
   YMNX HWDUYTLWFR NX JFXD YT IJHNUMJW.

2. This was entitled "Cold Country". It was encrypted using a monoalphabetic substiution cipher. Decipher it.
   TOWWJPHJC ZY RXW PHOTWYR ZYPHJC ZJ RXW SFOPC. UFYR FB ZR ZY QFIWOWC SZRX ZQW RXFMYHJCY FB BWWR CWWD.

3. This is from some material from the NSA. First they wrote, "The history of cryptography dates to the Caesar cipher, where each letter is replaced by the letter three positions away in the alphabet."... Then this followed. What system was used for encryption and what does it say? VRRQ SHRSOH EHJDQ VOLGLQJ WKH DOSKDEHW EB DPRXQWV GLIIHUHQW WKDQ WKUHH WR GHWHUPLQH FLSKHU HTXLYDOHQWV.

4. Prove that modular addition and multiplication are associative.

5. What is the order of S_n, the symmetric group on n letters.

6. Prove that a cyclic group can have more than one generator.

7. Let G be a cyclic group of order n. Suppose $m \in \mathbb{Z}$, $m > 0$, and $m \mid n$. Prove that G contains exactly one subgroup of order m.

8. List the possible orders of the subgroups of $\mathbb{Z}_{35}^*$.

9. Let F be a field and x be a symbol (an *indeterminate*). Define the *ring of polynomials* in the indeterminate x to be

$$F[x] = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n \mid a_i \in F \ \forall i, \text{ and } n \geq 0\}$$

Addition and multiplication are defined as follows:

- If $p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ and $q(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$, then $p(x) + q(x) = c_0 + c_1x + c_2x^2 + ... + c_kx^k$, where $c_i = a_i + b_i$ for all i (any a_i or b_i which is not explicitly listed is zero).
- If $p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ and $q(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$, then $p(x) \bullet q(x) = c_0 + c_1x + c_2x^2 + ... + c_kx^k$, where

$$c_i = a_i \bullet b_0 + a_{i-1} \bullet b_1 + ... + a_0 \bullet b_i$$

for all i (any a_i or b_i which is not explicitly listed is zero).

Prove that $F[x]$ is a ring.

10. List all elements of $\mathbb{Z}_{15}^*$ along with their orders and inverses.

11. Find a subgroup of order 4 in $\mathbb{Z}_{15}^*$, and a subgroup of order 6 in $\mathbb{Z}_{21}^*$.

12. Try using Maple. The command to start up a Maple session is **xmaple**. The **Help** menu is on the toolbar. From there, get to **New Users** and then **Quick Tour**. Begin reading that (if the system you are on lets you choose between various tours, the first nine sections and section 17 of the Quick Tour are useful). Try typing `?igcdex` to get help on Maple's function for the Extended Euclidean Algorithm. Note that, rather than just reading, you can actually execute the Maple statements in the Tour, as you read. Try some examples and check that the values you get are correct. We will be using Maple later in the course to do calculations which are hard (or impossible) to do by hand.