Institut for Matematik og Datalogi September 5, 2016
Syddansk Universitet JFB

Cryptology – E16 – Lecture 1

Textbook

Nigel P. Smart, *Cryptography Made Simple*, Springer, 2016. 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 12:15 on Mondays, 10:15 on Tuesdays, and 8:15 on Wednesdays, in the seminar room. The first two classes will be lectures, but after that we will alternate between lectures and discussion sections. Some classes will be cancelled, since this leads to more than listed in the course description. Be alert for announcements for cancellation.

There will be assignments which must be approved in order to take the oral exam in January. The assignments are considered "exam projects". Thus, you may not work with anyone not in your group, but you may work in groups of two to three students. The assignments must be turned in on time. There will be a chance to redo at most two assignments (of the four or five), if they are either late or not good enough the first time. The assignments must be turned in through Blackboard, as one PDF file. Make sure the names of everyone in your group appears on the cover page, or at the top of the first page. Turn in only one copy per group.

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

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

My office hours will be Tuesdays and Thursdays from 9:00 to 9:45.

Lecture, September 5

We will begin with an introduction to the course. Then, we will cover sections 7.1–7.2, plus some definitions of the parts of a cryptosystem on page 164. We may also cover the Vigenere cipher if there is time.

Lecture, September 6

We will cover section 1.1 on algebra. There are more notes on this on the course homepage, along with some slides. In the discrete math notes, algebra starts on page 6. In addition, you should read about the Extended Euclidean Algorithm and the Chinese Remainder Theorem (section 1.3 in the textbook) if you are not familiar with them or need a review.

Problem session September 7

Note that those problems we cannot finish on September 7 will be done in the next discussion section, September 13.

1. This was encrypted using a shift cipher. Decipher it.
   NBCM CM HIN PYLS BULX.

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 (see the notes).

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 **Take a Tour of Maple** and then **10 Minute Tour**. Begin reading that (if the system you are on lets you choose between various tours, the sections on graphics, differential equations and units of measurement are less interesting for the purposes of this course). 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.