Institut for Matematik og Datalogi
Syddansk Universitet

February 17, 2005
JFB

Cryptology – F05 – Lecture 3

Lecture, February 11

We began with an introduction to the course. Then, we covered sections 1.1.1–1.1.4 and 1.2.1–1.2.3 in the textbook.

Lecture, February 16

We covered the discrete math notes on algebra (starting on page 181) from the home page for the course, plus those on the Extended Euclidean Algorithm (section 5.2.1 in the textbook).

Lecture, February 18

We will continue with chapter 1 in the textbook, skipping the Hill Cipher and begin on chapter 2.

Lecture, February 25

We will finish with chapter 2.

Problem session February 23

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. Suppose you had two examples of ciphertext, both enciphered using periodic polyalphabetic ciphers. How would you make an intelligent guess as to whether or not the same sequence of substitution alphabets was used, without making any attempt at deciphering? Is the assumption that the ciphers are periodic necessary?

5. During lecture I stated that a linear feedback shift register sequence produced by a recurrence of degree n has period at most $2^n - 1$. Prove that the period cannot be longer than this. (Hint: consider the set of different values which could be in the register while the sequence is being produced.)

6. Suppose that a linear feedback shift register sequence is produced by a recurrence of degree n and has period $2^n - 1$. In general, exactly how many zeros are there among the first $2^n - 1$ bits produced. Prove your answer.

7. Prove that modular addition and multiplication are associative.

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

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

10. 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.

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

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

$$F[x] = \{a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \mid a_i \in F \ \forall i, \text{ and } n \geq 0\}$$

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.

13. Try using Maple. The command to start up a Maple session is **xmaple**. The **Help** menu is in the upper righthand corner. From there, get the **New User's 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. Try some examples and check that the values you get are correct.

Assignment due Friday, March 4, 10:15 AM

Note that this is part of your exam project, so it must be approved in order for you to take the exam in June, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become the assignment you redo). You may work in groups of two or three.

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

2. Consider multiple round Vigenère encryption, both in the case where all periods are the same length and in the case where they might have different lengths. Multiple round encryption is encryption more than once, using a different key for each encryption. (The ciphertext from round i is the plaintext input to round $i + 1$). Is there any security advantage to multiple round encryption in the different cases? How could such a system be cryptanalyzed?

3. Suppose that you are able to obtain the cyphertext "01101010101101", and you learn that the first eight bits of the plaintext are "11011001". You know that the encryption was done with the aid of a linear feedback shift register over the field GF(2), with length four. Determine the linear feedback shift register and the remainder of the message.

4. The known-plaintext attack on the linear feedback shift register stream cipher discussed in the textbook requires n bits of plaintext and n corresponding bits of cipher text where $n = 2m$ (and the recurrence has degree m) to reconstruct the entire key stream. Suppose that instead of $2m$ bits of plaintext and corresponding ciphertext, the cryptanalyst has only $2m - 3$ bits. How would this cryptanalyst reconstruct the entire key stream? Can the cryptanalyst be certain of getting the correct answer?

5. Suppose that a keystream S is produced by a linear feedback shift register with n stages (by a linear recurrence relation of degree n). Suppose the period is $2^n - 1$. Consider any positive integer i and the following triples of positions in S:

$$(S_i, S_{i+1}, S_{i+2}), (S_{i+1}, S_{i+2}, S_{i+3}), ..., (S_{i+2^n-2}, S_{i+2^n-1}, S_{i+2^n}).$$

How many of these triples are such that $(S_j, S_{j+1}, S_{j+2}) = (1, 1, 1)$? (In other words, how many times within one period does the pattern 111 appear?)

Prove that your answer is correct.