Institut for Matematik og Datalogi
Syddansk Universitet

February 10, 2003
JFB

Cryptology – F03 – Lecture 3

Textbook

Lecture, February 4

We began with an introduction to the course. Then, we covered sections 1.1.1–1.1.3 and 1.2.1–1.2.2 in the textbook.

Lecture, February 6

We covered the discrete math notes on algebra (pages 6–12) from the home page for the course.

Lecture, February 11

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

Problem session February 13

We will talk about problems 1, 2, 3, 7, and 8. There will probably be extra time and I will lecture on the Extended Euclidean Algorithm and the Chinese Remainder Theorem.

Lecture, February 18

We will finish chapter 2 in the textbook.

Assignment due Thursday, February 27, 8:15 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. If it is late, it will not be accepted.

1. List all elements of $\mathbb{Z}_{11}^*$ along with their orders and inverses. Which elements are generators of $\mathbb{Z}_{11}^*$?

2. Do problem 1.20 in the textbook.

3. Do problem 1.29 in the textbook.

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 $2m - 2$ bits. How would this cryptanalyst reconstruct the entire key stream?

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 pairs of positions in S:

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

   How many of these pairs are such that $(S_j, S_{j+1}) = (1, 1)$? (In other words, how many times within one period does the pattern 11 appear?)

   Prove that your answer is correct.

Problems for Thursday, February 20

1. Do problems 3, 4, 5, and 6 from the last set of problems.

2. Prove that modular addition and multiplication are associative.

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

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

5. 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.

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

7. 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.