Institut for Matematik og Datalogi
Syddansk Universitet

February 9, 2011
JFB

Cryptology – F11 – Week 3

Lecture, February 8

We covered section 1.1.7 and 1.2.5 in chapter 1 of the textbook. Then we covered most of chapter 2, but we skipped Huffman coding, which is covered in DM507.

Lecture, February 11

We will finish chapter 2 by covering Theorem 2.4. Then, we will cover chapter 3 in the textbook, skipping most of the first four sections. The original Rijndael specification (which can be found through the course's homepage) will be used as the basis for the description of AES.

Lecture, February 16

We will finish chapter 3 in the textbook and begin on chapter 5. We will skip section 5.2.1 on the Extended Euclidean Algorithm.

Problem session February 15

1. 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.)

2. 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.

3. Problem 1.20 in the textbook. Note that to be periodic, you don't have to start from the beginning, just be ultimately periodic.

4. Suppose that you are able to obtain the ciphertext "01100111101001", and you learn that the first eight bits of the plaintext are "10110110". 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.

5. Problem 2.4 in the textbook.

6. Problem 2.10 in the textbook.

Problem session February 18

1. Problem 2.11 in the textbook.

2. Problem 2.17 in the textbook.

3. 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.

4. Problem 3.3 in the textbook.

5. Problem 3.7 in the textbook.

Assignment due Tuesday, March 1, 12:15

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. Consider the multiplicative group $\mathbb{Z}_n^*$, where n is prime and $n-1 = 3s$ for some integer s.

   a. Prove that the set, $H = \{g^3 \mid g \in \mathbb{Z}_n^*\}$ is a subgroup of G.

   b. Prove that there exists some $g \in \mathbb{Z}_n^* \setminus H$.

   c. Prove that $|H| \leq |\mathbb{Z}_n^*|/2$.

2. The substitution cipher defined in section 1.1.2 of the textbook is sometimes referred to as a *monoalphabetic substitution cipher*, while the Vigenère cipher of section 1.1.4 is referred to as a *polyalphabetic substitution cipher*. With a monoalphabetic substitution cipher, the same permutation of the alphabet is used for the entire message and is the key. For a polyalphabetic substitution cipher, some number, d, of permutations of the alphabet are used, giving d different keys, k_1, k_2,...,k_d. These keys are then used periodically to encrypt the message. In the specific case of the Vigenère cipher, all of the permutations are simply cyclic shifts, but this is not necessary more generally. Consider these more general polyalphabetic substitution ciphers. What techniques from chapter one in the textbook can be used towards breaking these systems? Explain your answer. If there are any techniques from section 1.2.3 which you cannot use, also explain why not.

3. Suppose a plaintext alphabet, P, and a ciphertext alphabet, C, are both equal to G, where G is a finite group with group operation $\odot$. Consider the following symmetric key cryptosystem. A message $m = m_1 m_2 \ldots m_s$, consisting of s symbols from P is encrypted using a shared secret key, $K = k_1 k_2 \ldots k_s$, consisting of s values chosen randomly, uniformly and independently from G. Symbol m_i from the message is encrypted using k_i, giving the result $c_i = k_i \odot m_i$. A key is never used more than once.

   a. How is decryption performed? Does it matter if G is commutative?

   b. Show that this cryptosystem has perfect secrecy.

   c. What advantage or disadvantage does this system have over the one-time pad defined in the textbook?

4. 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.

5. Suppose that a keystream S is produced by a linear feedback shift register with m stages (by a linear recurrence relation of degree m).

a. Assume that S does not end with an infinite string of alternating zeros and ones. What is the longest string of alternating zeros and ones which could appear in S? Prove your answer.

b. Prove that it is possible for such a keystream S produced by an m-stage linear feedback shift register to have a period of $< m$, but at least 5 (for some $m > 6$).