Institut for Matematik og Datalogi
Syddansk Universitet

February 21, 2013
JFB

Cryptology – F13 – Week 3

Lecture, February 7

We covered linear feedback shift registers from chapter 1 in the textbook. Then we covered chapter 2, skipping Huffman coding, which is covered in DM507.

Lecture, February 11

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 15

We will begin on chapter 5 in the textbook, skipping the Extended Euclidean Algorithm, because you should already know it.

Problem session February 14

1. 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.

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

3. 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.

4. Problem 2.4 in the textbook.
5. Problem 2.10 in the textbook.
6. Problem 2.11 in the textbook.
7. Problem 2.17 in the textbook.
8. I may lecture at the end.

Problem session February 18

1. 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.

2. Problem 3.3 in the textbook.
3. Problem 3.7 in the textbook.
4. I may lecture at the end.

Assignment due Friday, March 1, 10:00

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). Turn

in the assignment through the SDU Assignment system in Blackboard, and remember to keep your receipt. Turn in one PDF file per group.

1. 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.

2. Consider a linear feedback shift register with 4 stages (a linear recurrence of degree 4), where the tap sequence is $c_0 = c_3 = 1, c_1 = c_2 = 0$. Suppose a sequence of $4n$ random bits $b_1, b_2, ..., b_{4n}$ is partitioned into consecutive substrings of length 4. For each substring, the linear feedback shift register is applied in such a way that the first output bit (which is also the first bit of the input to the linear feedback shift register) is ignored and the next four output bits are placed in a new sequence. For example, if the original random sequence is 10100111, then the new sequence is 01011111, where the 4th and 8th bits were computed by the linear feedback shift register and the others are just rotates to the left.

   a. Suppose the original sequence is 11001001. What is the new sequence produced?

   Suppose that a plaintext alphabet $P = \{0, 1\}$, so that a message m is a sequence of bits $(m_1, m_2, ..., m_s)$. Suppose that encryption of a message is bitwise XOR with the new sequence produced from a random original sequence (as with a one-time pad, but the bits for encryption are from the new sequence, not the random original sequence).

   b. Suppose the sender and receiver of the encrypted message share the random original sequence and both know the tap sequence. How does the receiver decrypt?

   c. Show that this cryptosystem has perfect secrecy.

d. Suppose that the tap sequence is changed so that $c_0 = c_2 = c_3 = 0$ and $c_1 = 1$. Explain why the cryptosystem now does not have perfect secrecy.

3. Consider a cyclic group G, where $|G| = 5s$ for some integer s.

   a. Prove that the set, $H = \{g^5 \mid g \in G\}$ is a subgroup of G.

   b. Prove that there exists some $g \in G \setminus H$.

   c. Prove that $|H| \leq |G|/2$.

   d. Suppose you did not know a generator of G, but knew $|G|$. How could you efficiently test for some element $h \in G$ whether or not $h \in H$? (Hint: Assume that multiplication in G can be done efficiently. Then, raising h to any power less than $|G|$ can be done efficienlty using fast exponentiation.) Explain why your test works and why it is efficient.

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?