

## Cryptology – F08 – Week 2

### **Lecture, January 28**

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 and almost finished covering the Vigenere cipher.

### **Lecture, January 31**

We covered the discrete math notes on algebra (starting on page 6 of the notes or 181 of the slides) from the home page for the course. You should also read those on the Extended Euclidean Algorithm (section 5.2.1 in the textbook).

### **Lecture, February 4**

We will continue with chapter 1 in the textbook, skipping the Hill Cipher and cover chapter 2. We will skip Huffman coding, which is covered in DM507.

### **Lecture, February 8**

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.

### **Problem session February 7**

1. Find all elements of the subgroup of  $\mathbb{Z}_{35}$  generated by 8 and 27.
2. Which elements are generators of  $\mathbb{Z}_{11}^*$ ?

3. 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?
4. 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.)
5. 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.
6. In the multiplicative group module  $n$ ,  $\mathbb{Z}_n^*$ , an important subgroup we will be studying is the the quadratic residues. A number  $x \in \mathbb{Z}_n^*$  is a quadratic residue module  $n$  if and only if it can be written as a square,  $x = y^2 \pmod{n}$ . For example, 2 is a quadratic residue modulo 7, since  $2 = 3^2 \pmod{7}$ .
  - (a) List the quadratic residues modulo 15.
  - (b) Show that for any number  $n$ , the set of quadratic residues modulo  $n$  is a subgroup of  $\mathbb{Z}_n^*$ .
7. Do problem 1.20 in the textbook. Note that to be periodic, you don't have to start from the beginning, just be ultimately periodic.
8. 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  $\text{GF}(2)$ , with length four. Determine the linear feedback shift register and the remainder of the message.

### Assignment due Friday, February 22, 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. Let  $G$  be a cyclic group of order  $n$ . Suppose  $m \in \mathbb{Z}$ ,  $m > 0$ , and  $m \mid n$ .  $G$  contains exactly one subgroup,  $H$ , of order  $m$ , and raising an element  $g \in G$  to the power  $n/m$  gives an element  $h \in H$ .
  - a. Give a value  $s$ , expressed as a function of  $m$  and/or  $n$ , with  $2 \leq s \leq n - 1$ , such that for every  $g \in G$ ,  $g^{\frac{n}{m}} = (g^s)^{\frac{n}{m}}$ ?
  - b. For a given  $h \in H$ , how many  $g \in G$  are such that  $h = g^{\frac{n}{m}}$ ? Prove your answer.
  
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 a plaintext alphabet,  $P$ , and a ciphertext alphabet,  $C$ , are both equal to  $Z_p^*$ , where  $p$  is an odd prime. Consider the following symmetric key cryptosystem. A message  $m = m_1 m_2 \dots m_s$ , consisting of  $s$  symbols from  $P$  is encrypted using a shared secret key,  $K = k_1 k_2 \dots k_s$ , consisting of  $s$  values chosen randomly, uniformly and independently from  $Z_p^*$ . Symbol  $m_i$  from the message is encrypted using  $k_i$ , giving the result  $c_i = m_i \cdot k_i \pmod{p}$ . A key is never used more than once.
  - a. How is decryption performed?
  - 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  $S$ :

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

How many of these pairs are such that  $(S_j, S_{j+1}) = (0, 1)$ ? (In other words, how many times within one period does the pattern 01 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  $m$ ).

Prove that it is possible for such a keystream  $S$  produced by an  $m$ -stage linear feedback shift register to have a period of  $m$ .