

## Cryptology – F11 – Week 2

### Lecture, February 1

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 2

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. In addition, you should read about the Extended Euclidean Algorithm (section 5.2.1 in the textbook) if you are not familiar with it or need to review it.

### Lecture, February 8

We will cover section 1.1.7 and 1.2.5 in chapter 1 of the textbook. Then we will cover chapter 2, but we will skip 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.

### Problem session February 9

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. Show that the intersection of the subgroups,  $H_1$ ,  $H_2$ , and  $H_3$  of a group  $G$  is also a subgroup of  $G$ .
4. In the multiplicative group modulo  $n$ ,  $\mathbb{Z}_n^*$ , an important subgroup we will be studying is the the quadratic residues. A number  $x \in \mathbb{Z}_n^*$  is a quadratic residue modulo  $n$  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  $\mathbb{Z}_n^*$ .
5. 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?