

Cryptography – 2019 – Lecture 2

Lecture, September 2

We began with an introduction to the course. Then, we covered sections 7.1–7.4, plus some definitions of the parts of a cryptosystem on page 164.

Lecture, September 3

We will cover section 1.1 on algebra. There are more notes on this on the course homepage, along with some slides. In the discrete math notes, algebra starts on page 6. In addition, you should read about the Extended Euclidean Algorithm and the Chinese Remainder Theorem (section 1.3 in the textbook) if you are not familiar with them or need a review.

Lecture, September 9

We will cover chapter 9 and section 11.2, including the proof of Lemma 2.3 and the birthday bound at the top of page 24.

Problem session September 10

1. Suppose you had two examples of ciphertext, both enciphered using Vigenère ciphers. How would you make an intelligent guess as to whether or not the same sequence of substitution alphabets was used, without directly attempting to decipher? Is the assumption that the key stream is periodic (as in the Vigenère cipher) necessary?
2. Find all elements of the subgroup of \mathbb{Z}_{35} generated by $\{8, 27\}$.
3. Which elements are generators of \mathbb{Z}_{11}^* ?

4. Show that the intersection of the subgroups, H_1 , H_2 , and H_3 of a group G is also a subgroup of G .
5. 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 integer $n \geq 3$, the set of quadratic residues modulo n is a proper subgroup of \mathbb{Z}_n^* .
 - (c) Show that the set of quadratic residues modulo n , n an odd prime, is the set of elements, x , of \mathbb{Z}_n^* such that $x^{\frac{n-1}{2}} \equiv 1 \pmod{n}$.
 - (d) Give a randomized algorithm for finding an element which is not a quadratic residue modulo an odd prime n , where the probability of success is at least $1/2$ in each attempt.