Lecture 4: Finite Fields (PART 1)

PART 1: Groups, Rings, and Fields

Theoretical Underpinnings of Modern Cryptography

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

January 23, 2017
11:29pm

Goals:

- To answer the question: Why study finite fields?
- To review the concepts of groups, rings, integral domains, and fields

CONTENTS

4.1: WHY STUDY FINITE FIELDS?

- It is almost impossible to fully understand practically any facet of modern cryptography and several important aspects of general computer security if you do not know what is meant by a finite field.

- For example, without understanding the notion of a finite field, you will not be able to understand AES (Advanced Encryption Standard) that we will take up in Lecture 8. As you will recall from Lecture 3, AES is supposed to be a modern replacement for DES. The substitution step in AES is based on the concept of a multiplicative inverse in a finite field.

- For another example, without understanding finite fields, you will NOT be able to understand the derivation of the RSA algorithm for public-key cryptography that we will take up in Lecture 12.

- And if you do not understand the basics of public-key cryptography, you will not be able to understand the workings of several modern protocols (like the SSH protocol you use everyday for

logging into other computers) for secure communications over networks. You will also not be able to understand what has become so important in computer security — *user and document authentication with certificates*.

- Another modern concept that will befuddle you if you do not understand public key cryptography is that of *digital rights management*. And, as I mentioned earlier, you cannot understand public key cryptography without coming to terms with finite fields.

- For yet another example, without understanding finite fields, you will never understand the up and coming ECC algorithm (ECC stands for Elliptic Curve Cryptography) that is already in much use and that many consider to be a replacement for RSA for public key cryptography. We will take up ECC in Lecture 14.

- As you yourself can see, if you do not understand the concepts in this and the next three lectures, you might as well give up on learning computer and network security.

- To put it very simply, a finite field is a finite set of numbers in which you can carry out the operations of addition, subtraction, multiplication, and division without error. In ordinary computing, division particularly is error prone and what you see is

a high-precision approximation to the true result. Such high-precision approximations do not suffice for cryptography work. All arithmetic operations must work without error for cryptography.

- The stepping stones to understanding the concept of a finite field are:

  1. *set*
  2. *group*
  3. *abelian group*
  4. *ring*
  5. *commutative ring*
  6. *integral domain*
  7. *field*

- In the next section, we start with the notions of *set* and *group*.