Scribe: Cryptography and Network Security (Week 6 Class 4)

Aditya Anand

12-Oct-2020

1 Introduction

In the previous lectures we discussed extensively the DES encryption scheme, and the need for 3DES encryption. However, 3DES came with its set of limitations. Two of them, in particular, are of significance - the algorithm is sluggish in software, and the block size is only 64 bits (brute force attacks, though unlikely, maybe a concern). After several rounds of competitions, the Rjindael algorithm was selected as the AES algorithm, with better security guarantees compared to 3DES. In this lecture, we focussed on developing techniques and results on finite fields as a precursor for discussing AES encryption. We discuss the construction and properties of finite fields. Finite fields are widely used in various encryption schemes.

2 Finite fields

We recall the definition of a field.

Definition 1. *A field is a set S with two binary operations $+, *$, such that*

1. *$(S, +)$ is an abelian group.*
2. *$(S \setminus \{0\}, *)$ is an abelian group, where 0 is the additive identity*
3. *The operation $*$ distributes over $+$.*

A field $(S, +, *)$ is *finite* if S is finite, and finite fields are also called *Galois* fields. For a finite field $F = (S, +, *)$, the number of elements in S is called the *order* of the field F. For a simple example of a finite field, consider the finite field $\mathbb{F}_2$ on the set $\mathbb{Z}_2 = \{0, 1\}$. The addition $(+)$ operation is addition modulo 2, and the multiplication operation (*) is multiplication modulo 2. This example readily generalizes to the field $\mathbb{F}_p$ with the set $\mathbb{Z}_p = \{0, 1, ...p - 1\}$, where the operations are addition and multiplication modulo p, for a prime number p. However notice that the set $\mathbb{Z}_n$, with the operations as addition and

multiplication modulo n does not form a field for composite n, since an element a for which $gcd(a, n) \neq 1$ does not have a multiplicative inverse modulo n.

As we understand from the preceeding example, the properties of a finite field are quite strong, and we may guess that the structure of these fields must therefore be restricted. The following well-known result confirms this suspicion.

Theorem 1. *The order of any finite field must be of the form p^n for some prime p and $n \in \mathbb{N}$.*

Next we define the characteristic of a field.

Definition 2. *Given a field $(S, +, *)$, the* characteristic *of F is the smallest positive integer λ such that for any $a \in S$, $\lambda a = a + a + a....$ repeated λ times $= 0$.*

We state the following lemma without proof.

Lemma 1. *The characteristic of a finite field with p^n elements, where p is a prime, $n \in \mathbb{N}$ is p.*

3 Polynomials and fields of non-prime order

Recall that earlier we studied that every finite field has an order which is a power of a prime. But the only fields we have considered so far are the fields $\mathbb{F}_p$ where p is prime. In this section our goal is to construct finite fields of order p^x where $x > 1$. We need a few more definitions before we describe the construction.

Given a field F, we define a polynomial in F as a polynomial where each coefficient is from F. The set of all polynomials on the variable x in the field F is denoted by $F[x]$. Addition of polynomials is regular addition keeping each coefficient modulo 2. As an illustration, consider the polynomials $a(x) = x + 1$, $b(x) = x^2 + 1$, $a, b \in \mathbb{F}_2[x]$. The addition $a(x) + b(x) = x^2 + x + 1 + 1 = x^2 + x$, since $1 + 1 = 0$ in $\mathbb{F}_2$ arithmetic. Multiplication of polynomials in finite fields is more tricky. One natural extension that comes to our mind is to take the result of regular multiplication modulo a polynomial of some degree m, thus maintaining the result with degree less than m.

However, such an approach may not work, since we must be careful to make sure that multiplicative inverses exist. Recall that the ring $\mathbb{Z}_n$ is a field only when n is prime. With this motivation, we proceed to define a notion of "prime" polynomials in a field, called irreducible polynomials.

Definition 3. *A polynomial $d(x)$ is irreducible in a field F, if there are no two non-constant polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $d(x) = a(x)b(x)$ (following the arithmetic of field F).*

To define the multiplication operation on $F[x]$, where F is a finite field , we first fix an irreducible polynomial $m(x)$ in $F[x]$. Then the multiplication of two polynomials $a(x)$ and $b(x)$, is their polynomial multiplication, taken modulo the polynomial $m(x)$ (of course, the coefficients follow the arithmetic of F).

Now we describe the construction of a field with p^n elements, $n > 1$. Consider the field $\mathbb{F}_p$. Fix an irreducible polynomial $m(x)$ of degree n in $\mathbb{F}_p[x]$ (it is known that such polynomials always exist for every $n \in \mathbb{N}$, we shall not prove that in this class). Now consider the field whose underlying set consists of all polynomials of degree less than n in $\mathbb{F}_p[x]$. Clearly the size of this set is p^n. The addition operation is the addition of polynomials keeping coefficients modulo p, and the multiplication operation is the polynomial multiplication where coefficients are kept modulo p, taken modulo $m(x)$. It is easy to check that all the field properties are satisfied, and in particular multiplicative inverses exist for all non-zero elements by the way we have defined the polynomial $m(x)$.

In particular, our construction shows that for every prime p and positive integer n there is a finite field with p^n elements. We denote a field on p^n elements as $GF(p^n)$. For an example to understand how the construction works, consider the field $GF(2^3)$. Here $n = 3$, so we must choose an irreducible polynomial of degree 3 in $\mathbb{F}_2$. $x^3 + x + 1$ is one such polynomial (it is easy to verify it is irreducible in $\mathbb{F}_2$). The elements of $GF(2^3)$ are now represented by the polynomials of degree less than 3, i.e. the elements $\{0, 1, x, x+1, x^2+1, x^2+x+1, x^2+x, x^2\}$.

For the sake of completeness, let us show formally that x^3+x+1 is irreducible in $\mathbb{F}_2[x]$. Suppose to the contrary, that it is not. Then it follows that it splits into two factors, and that atleast one factor must have degree 1. A degree 1 term of the form $x - a$ can divide $x^3 + x + 1$ only when $a^3 + a + 1 = 0$. Since $0^3+0+1 \neq 0$ and $1^3+1+1 \neq 0$, it cannot happen that x^3+x+1 has a degree-1 factor in $F_2[x]$, and thus $x^3 + x + 1$ is irreducible in $\mathbb{F}_2$.

4 Introduction to AES (Advanced Encryption Standard)

This section provides a brief introduction to AES, we will cover the details of AES in the forthcoming classes. As mentioned before, 3-DES has certain drawbacks, including the fact that it is sluggish in software and uses only a 64-bit block size. For these reasons, it was decided that a more robust and secure encryption scheme was needed. The NIST announced the need for a new encryption scheme in 1997. In 2001, after an international competition, in which multiple algorithms which reached the finals were deemed fit for secure encryption, the AES (Advanced Encryption Standard) was chosen as the Rjindael scheme, proposed by Belgian cryptographers Vincent Rjimen and Joan Daemen. Here we note that there are minor differences between the adopted AES and the originial Rjindael scheme, and we shall discuss the details of the former.

The AES uses a 128-bit block size, and the key-size is either 128, 192, or 256 bits (called AES-128, AES-192, AES-256 respectively). AES-128, 192, and 256 apply 10,12 and 14 rounds of encryption respectively. On a high level, the algorithm arranges the 128 bits (or 16 bytes), in a $4 * 4$ grid, where each

grid contains a single byte. Then various operations are applied to this grid. Some of these including re-distributing information across rows, columns, and performing substitutions. We shall go into the details of the AES algorithm in the forthcoming classes.

5 Conclusion

In this lecture we studied various properties of finite fields pertaining to their structure and construction. We considered the construction of fields on p^n elements, where p is a prime and n is a positive integer, and showed how to construct such a field from the set of polynomials of degree less than n with coefficients in $\mathbb{F}_p$. Finally, we had a brief introduction to AES encryption.