Justin Ciocoi

Oct 3, 2023

CSCI 360 Notes

Cryptography and Cryptanalysis

Fields

Basic Definition of Fields

- **Wiki Definition:**
  - In mathematics, a field is a set on which addition, subtraction, multiplication, and division are defined and behave as the corresponding operations on rational and real numbers do.
- A field is a set of numbers or expressions that must satisfy the following conditions:
  - Associativity of addition and multiplication across the set
    - $a + (b + c) = (a + b) + c$
    - $a * (b * c) = (a * b) * c$
  - Commutativity of addition and multiplication across the set
    - $a + b = b + a$
    - $a * b = b * a$
  - Existence of additive and multiplicative identities i.e.
    - There exists 0 and 1 such that
      - $a + 0 = a$
      - $a * 1 = a$
  - Existence of Unique Additive Inverses
    - for every a in the field, there exists a^{-1} such that $a + a^{-1} = 0$
  - Existence of Multiplicative Inverses
    - for every nonzero a in the field, there exists a^{-1} such that $a * a^{-1} = 1$
    - 0 is excluded, since 0 *cannot* have a multiplicative inverse, since anything multiplied by 0 is 0, and can never be 1
  - Distributivity of multiplication over addition
    - $a * (b + c) = (a * b) + (a * c)$
- For any prime integer n, the set of integers in $\mathbb{Z} \mod n$ is a finite field

- An extension is a field that contains all the elements of the finite field but is not the finite field itself

Overview of Fields

- The following is a description of fields from the Understanding Cryptography textbook
- First, let us define a **group**
  - A set of elements with an operation, $\circ$, which combines two elements of the group, and must satisfy each of the following properties
    - The operation $\circ$ is closed
      - for all $a, b \in G$ it holds that $a \circ b = c \in G$
    - The operation is associative
      - for all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$
    - There is an identity element, I
      - for all $a \in G$ there exists I, such that $a \circ I = I \circ a = a$
    - There is an inverse element a^{-1}
      - for all $a \in G$ there exists a^{-1} such that $a \circ a^{-1} = a^{-1} \circ a = 1$
    - Commutativity
      - for all $a, b \in G$, $a \circ b = b \circ a$
  - Roughly speaking, a group is a set with one operation
  - The operation used in the above definition, $\circ$, can be any of the 4 basic operations $(+, -, *, \div)$
    - However, we can instead use additive inverses and multiplicative inverses to replace subtraction and division
- Now, with the definition of a **group**, we can move on to the definition of a **field**
- We can define a **field**, F, as a set of elements that satisfies the following properties
  - All elements of F form an additive group with the group operation $+$ and the neutral element 0

    - All elements of F form a multiplicative group with the group operation $*$ and the neutral element 1
    - When the two group operations are mixed, the distributivity law holds, i.e.
        - for all $a, b, c \in F : a(b + c) = (a * b) + (a * c)$
    - For example, the set of all real numbers, $\mathbb{R}$, is a **field**
- There are an infinite number of fields with an infinite number of elements, but for the purposes of cryptography, we are more interested in fields with a finite set of elements
- Finite fields are also known as **Galois Fields**
- A field of order m only exists if m is a prime power
    - This means $m = p^n$ for some positive integer n and a prime integer p
    - The prime number p is called the **characteristic** of the field

Prime Fields

- A prime field is a finite field as defined above, with the positive integer $n = 1$
- Now, let p be a prime number
    - The integer ring $\mathbb{Z}_p$ can be denoted as $GF(p)$ and is referred to as a prime field, or a **Galois Field** with a prime number of elements
    - All nonzero elements of $GF(p)$ have an inverse
    - Arithmetic in $GF(p)$ is done in modulo p

Extension Fields

- Let us look at an example of **Extension Fields**
- Extension fields, $GF(2^m)$ elements are represented as polynomials rather than as integers
- So, for example, in **AES**, where the field $GF(2^8)$ is used, each element $A \in GF(2^8)$ can be represented as a polynomial in the form
    - $A(x) = a_7x^7 + ... + a_1x^1 + a_0$
    - where $a_i \in GF(2) = 0, 1$
    - Since the coefficients are only 0s and 1s, we can store the polynomial in an 8-bit vector of the following form rather than storing the entire polynomial
        - $A = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$

- *Operations in Extension Fields*
  - Let $A(x), B(x) \in GF(2^m)$
  - The sum of two elements can be computed according to
    - $C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i$
    - $c_i \cong (a_i + b_i)\%2$
  - The difference can similarly be computed according to
    - $C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i$
    - $c_i \cong a_i - b_i = (a_i + b_i)\%2$
  - Now, for multiplication we must also make the assumption that $P(x) \cong \sum_{i=0}^{m} p_i x^i$ for $p_i \in GF(2)$ is an irreducible polynomial
  - FOR **AES** The irreducible polynomial that is used is
    - $P(x) = x^8 + x^4 + x^3 + x + 1$
    - This is a part of the **AES Specification**
  - Now, we can perform multiplication on two elements using the following formula
    - $C(x) \cong (A(x) * B(x))\%P(x)$
    - In essence, this means you must multiply the two polynomials $A(x)$ and $B(x)$ and then divide the resulting product, $C(x)$, by the irreducible polynomial, $P(x)$
      - The remainder of this division will be the result of $A(x) * B(x)$