[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Subham Rathi (202151163)

Winter 2023-2024
Lecture (Week 4)

Group

Introduction to Groups

Definition 1 (Group) *A group is a set G equipped with an operation $\cdot$ that satisfies the following properties:*

1. ***Closure**: For all $a, b \in G$, $a \cdot b \in G$.*
2. ***Associativity**: For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
3. ***Identity Element**: There exists an element $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$.*
4. ***Inverse Element**: For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Theorem 1 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.*

Proof: Consider the left cosets of H in G. These cosets form a partition of G, and each coset has the same order as H. Therefore, the order of H must divide the order of G. ■

Examples of Groups

1. The set of integers $\mathbb{Z}$ with addition forms a group.
2. The set of non-zero rational numbers $\mathbb{Q}^*$ with multiplication forms a group.
3. The symmetric group S_n, consisting of all permutations of n elements, is a group under composition.

Ring

Introduction to Rings

Definition 2 (Ring) *A ring is a set R equipped with two operations, addition $(+)$ and multiplication $(\cdot)$, such that R satisfies the following properties:*

1. *R is an abelian group under addition.*
2. ***Multiplication is Associative**: For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
3. ***Distributive Property**: For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Lemma 1 *In a ring R, for any $a, b \in R$, $(-a)b = a(-b) = -(ab)$.*

Proof: We have $(-a)b + ab = (-a + a)b = 0 \cdot b = 0$. Thus, $(-a)b = -(ab)$. Similarly, $a(-b) = -(ab)$. ■

Examples of Rings

1. The set of integers $\mathbb{Z}$ with usual addition and multiplication is a ring.
2. The ring of polynomials $R[x]$ with coefficients in a ring R is a ring.
3. The matrix ring $M_n(\mathbb{R})$ of all $n \times n$ matrices with real entries forms a ring.

Field

Introduction to Fields

Definition 3 (Field) *A field is a set F equipped with two operations, addition $(+)$ and multiplication $(\cdot)$, such that F satisfies the following properties:*

1. *F is a commutative group under addition.*
2. *$F \setminus \{0\}$ is a commutative group under multiplication, where 0 is the additive identity.*
3. ***Multiplication Distributes Over Addition**: For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Examples of Fields

1. The set of rational numbers $\mathbb{Q}$ is a field.
2. The field of real numbers $\mathbb{R}$ is a field.
3. The field of complex numbers $\mathbb{C}$ is a field.

Field Extension

Introduction to Field Extensions

Definition 4 (Field Extension) *Let F and K be fields, where F is a subfield of K. Then, K is called a field extension of F, denoted as K/F.*

Examples of Field Extensions

1. The field extension $\mathbb{C}/\mathbb{R}$ represents the extension of real numbers to complex numbers.
2. The field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ represents the extension of rational numbers by adding the square root of 2.
3. The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ represents a finite field extension, where $\mathbb{F}_{p^n}$ is a finite field with p^n elements.

Advanced Encryption Standard (AES)

Introduction to AES

Definition 5 (AES) *Advanced Encryption Standard (AES) is a widely-used symmetric encryption algorithm for securing data. It operates on blocks and supports key sizes of 128, 192, or 256 bits.*

AES Key Sizes

Remark 1 *AES supports three key sizes: 128 bits (AES-128), 192 bits (AES-192), and 256 bits (AES-256).*

AES-128

Remark 2 *AES-128 employs a 128-bit key for encryption, providing a good balance between security and performance.*

AES-192

Remark 3 *AES-192 uses a 192-bit key, enhancing security compared to AES-128, suitable for applications requiring a higher level of protection.*

AES-256

Remark 4 *AES-256 utilizes a 256-bit key, offering the highest level of security among the three variants, suitable for highly sensitive data.*