[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Shivam Pawar (202151148)

Winter 2023-2024
Lecture (Weak #4)

Introduction to Groups

Definition: A group is a set G equipped with an operation which 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): The order of H divides the order of G if G is a finite group and H is a subgroup of G.

Proof: H's left cosets in G. Each of these cosets has the same order as H, and together they create a partition of G. As a result, H's order must divide G's order.

Examples

1. A group is formed by the set of integers $\mathbb{Z}$ with addition.
2. The set of real numbers $\mathbb{R}$ forms a group under addition. The non-zero real numbers ($\mathbb{R}^*$) also form a group under multiplication.
3. The set of positive integers $\mathbb{Z}^+$ forms a group under multiplication.

Introduction to Rings

Definition: A ring is a set R equipped with two operations, addition and multiplication, with R satisfying 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 $a, b \in R$, $(-a)b = a(-b) = -(ab)$.
Examples:

1. The set of Gaussian integers, representing complex numbers of the form $a + bi$, where a and b are integers and i is the imaginary unit, forms a ring under complex number addition and multiplication.

2. The ring of polynomials with coefficients in the ring of integers, denoted as $\mathbb{Z}[x]$, is a ring under polynomial addition and multiplication.

3. The set of integers with usual addition and multiplication forms a ring.

Introduction to Fields

Definition: A field is a set F equipped with two operations, addition and multiplication, such that F satisfies the following properties:

1. Under addition, F is a commutative group.

2. Under multiplication, $F \setminus \{0\}$, where 0 is the additive identity, is a commutative group.

3. The Distribution of Multiplication Over Addition: $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$ are true for every $a, b, c \in F$.

Examples:

1. The set of rational numbers $\mathbb{Q}$ is a field.

2. The set of real numbers $\mathbb{R}$ is a field.

3. The set of complex numbers $\mathbb{C}$ is a field.

Introduction to Field Extension

Definition: Let two fields F and K, where F is a subfield of K. Then, K is called a field extension of F, denoted as K/F.

Examples:

1. The extension of real numbers to complex numbers is represented by the field extension $\mathbb{C}/\mathbb{R}$.

2. The extension of rational numbers by adding the square root of two is a field extension.

3. Where F_{p^n} is a finite field with p^n elements, the field extension F_{p^n}/F_p denotes a finite field extension.

Advanced Encryption Standard (AES)

Definition: Data security is achieved by using the symmetric encryption algorithm known as Advanced Encryption Standard (AES). It is block-based and supports 128-, 192-, or 256-bit key sizes.

AES Key Sizes

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

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

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

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