[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Archit Verma (202151192) — Lecture (Week 4)

Introduction to Groups

Definition 1 (Group): A group consists of a set G along with an operation $(\cdot)$ satisfying the following properties:

1. Closure: For any elements $a, b \in G$, their product $a \cdot b$ is also in G.
2. Associativity: For all $a, b, c \in G$, the operation is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Identity Element: There exists an element $e \in G$ such that for any $a \in G$, $a \cdot e = e \cdot a = a$.
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.

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 any $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
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 of Rings

1. The integers $\mathbb{Z}$ with conventional addition and multiplication form a ring.
2. The ring $R[x]$, which includes polynomials with coefficients from a ring R, constitutes a ring.
3. The collection $M_n(R)$, encompassing all square matrices of size $n \times n$ with real entries, serves as another example of a ring.
4. Consider the ring of Gaussian integers $\mathbb{Z}[i]$, comprising numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$.

Introduction to Fields

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

1. F is an abelian group under addition.
2. $F \setminus \{0\}$ forms an abelian 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 rational numbers $\mathbb{Q}$ constitute a field.
2. The real numbers $\mathbb{R}$ represent another example of a field.
3. The complex numbers $\mathbb{C}$ serve as yet another example of a field.
4. The field of Gaussian rationals, denoted $\mathbb{Q}(i)$, extends the rational numbers to include complex numbers of the form $a + bi$ where $a, b \in \mathbb{Q}$.

Introduction to Field Extensions

Definition 4 (Field Extension): A field extension K/F is formed when a field K contains a subfield F.

Examples of Field Extensions:

1. The extension $\mathbb{C}/\mathbb{R}$ represents the extension from real numbers to complex numbers.
2. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ results from adding the square root of 2 to the rational numbers.
3. The extension $\mathbb{F}p^n/\mathbb{F}_p$ constitutes 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) serves as a widely used symmetric encryption algorithm employed for securing data. It operates on blocks and supports key sizes of 128, 192, or 256 bits.

AES Key Sizes

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

AES-128

Remark 2: AES-128 utilizes a 128-bit key for encryption, striking a balance between security and performance. For example, it is commonly used in securing online communications.

AES-192

Remark 3: AES-192 enhances security compared to AES-128 by using a 192-bit key. It finds applications in scenarios requiring a higher level of cryptographic strength, such as financial transactions.

AES-256

Remark 4: AES-256 offers the highest security among the three variants by utilizing a 256-bit key. It is suitable for highly sensitive data, including government and military applications.