[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024

Scribed by: Sanidhya Kumar (202151138) — Lecture (Week 4)

1 Groups

We already saw what groups are. Let us quickly revise. A group $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following three axioms:

1. **Associativity**: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

2. **Identity Element**: There is an element $1 \in G$, called the identity element, such that $a * 1 = 1 * a = a$ for all $a \in G$.

3. **Inverse**: For each $a \in G$, there exists an element $a^{-1} \in G$, called the inverse of a, such that $a * a^{-1} = a^{-1} * a = 1$.

Note: A group G is abelian (or commutative) if, furthermore, $a * b = b * a$ for all $a, b \in G$.

1.1 Examples

1. $(G, *)$ where G is the set of all invertible matrices.

2. $(\mathbb{Z}, +)$

3. $(\mathbb{Z}, *)$

4. $(\mathbb{Z}, -)$

5. $(\mathbb{Q}, *)$

6. $(\mathbb{Q} - \{0\}, *)$

7. $(\mathbb{Z}_n, +_n)$

   Let's check if $(\mathbb{Z}_n, +_n)$ is a group or not where the set $\mathbb{Z}_n$ contains integers from 0 to $n-1$ (inclusive), and the operation $+_n$ is defined as $x +_n y = (x + y) \mod n$.

   - Checking for associativity:

   $$\begin{aligned} (x +_n y) +_n z &= (((x + y) \mod n) + z) \mod n \\ &= (x + (y + z) \mod n) \mod n \\ &= x +_n (y +_n z) \end{aligned}$$

     Hence, $(\mathbb{Z}_n, +_n)$ is associative.

   - Checking for identity: 0 is the identity element as $x +_n 0 = x = 0 +_n x$.

- Checking for inverse: For any x in $\mathbb{Z}_n$, the inverse of x is $n - x$, since:

$$\begin{aligned} x +_n (n - x) &= (x + (n - x)) \mod n \\ &= n \mod n \\ &= 0 \end{aligned}$$

  Thus, every element in $\mathbb{Z}_n$ has an inverse.

Therefore, $(\mathbb{Z}_n, +_n)$ is a group, and it's also an abelian group.

8. Let's check if $(\mathbb{Z}_n - \{0\}, *_n)$ is a group or not where the operation $*_n$ is defined as $(a, b) *_n (c, d) = (a *_1 c) \mod n \times (b *_2 d) \mod n$.

   - This operation is associative on the given set.
   - Identity Element: The identity element is $(1, 1)$.
   - Inverse Element: The inverse of an element (x, y), denoted as (x^{-1}, y^{-1}), exists only if $\gcd(x, n) = 1$ and $\gcd(y, n) = 1$. Hence, not every element in $(\mathbb{Z}_n - \{0\}) \times (\mathbb{Z}_n - \{0\})$ has an inverse under this operation.
     Hence, $(\mathbb{Z}_n - \{0\}, *_n)$ is a group if $\gcd(x, n) = 1$.

1.2 Subgroups

A non-empty subset H of a group $(G, *)$ is a subgroup of G if H is itself a group with respect to the operation $*$ of G. If H is a proper subset and a group with respect to $*$ of G and $H \neq G$, then H is called a proper subgroup of $(G, *)$. H will have the following properties:

1. $H \subseteq G$
2. H is itself a group with $*$

Do note that $(G, *)$ is a group because $a \in G$, $a * a \in G$, $a * a * a \in G$,

Here $*$ is just a notation for the operation which would be performed $a^i = a * a * a \cdots a \in G$. A group G is cyclic if there is an element $\alpha \in G$ such that for every $b \in G$, there is an integer i with $b = \alpha^i$. This α is called the generator of $(G, *)$. Order of an element $a \in G$, $O(a)$, is the least positive integer m such that $a^m = e$ (where e is the identity element of G).

1.2.1 An Example

Given – $O(a) = 5$, $a^5 = e$. So, $S = \{e, a, a^2, a^3, a^4\}$ will be a subgroup of G as:

- $S \subseteq G$ and
- $(S, *)$ is a group since it is associative, commutative, and has an inverse ($a^{-1} = a^4$ and so on).
- All elements in S are generated by a only. So, a is a cyclic subgroup of G.

Note: Every subset of G is not necessarily a subgroup.

1.2.2 Cyclic Subgroups

If G is a group and $a \in G$, then the set of all powers of a will form a cyclic subgroup generated by a and denoted by $\langle a \rangle$. Let G be a group and $a \in G$ be an element of finite order t, then $|\langle a \rangle|$ denotes the size of the subgroup generated by a and equals t.

1.2.3 Lagrange's Subgroups

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Since the order of the element generating the subgroup is equal to the cardinality of the subgroup, therefore, the order of the element also divides $|G|$.

Let $a \in G$ and $O(a)$ be the order of element a. Therefore,

$$S = \{a^0, a^1, a^2, \dots, a^{O(a)-1}\} = \langle a \rangle$$

$(S, *)$ is a subgroup of $(G, *)$.

From Lagrange's Theorem,

$$|H| \text{ divides } |G| \Rightarrow O(a) \text{ divides } |G|$$

1.3 Important Result

If the order of $a \in G$ is t, then the order of a^k is $t/\gcd(t, k)$.

$$\langle a \rangle = \{e, a, a^2, \dots, a^{O(a)-1}\}$$

$$\langle at \rangle = \{e, ar, a^2t, \dots, (at)^{O(at)-1}\}$$

$$B = at$$

$$\langle at \rangle = \langle b \rangle = \{e, b, b^2, \dots, b^{O(b)-1}\}$$

If gcd(t, O(a)) = 1, then O(at) = O(a)

2 Ring

A ring $(R, +_R, \times_R)$ consists of one set R with two binary operations arbitrarily denoted by $+_R$ (addition) and $\times_R$ (multiplication) on R satisfying the following properties:

1. $(R, +_R)$ is an abelian group with the identity element 0_R.
2. The operation $\times_R$ is associative, that is,
$$a \times_R (b \times_R c) = (a \times_R b) \times_R c \text{ for all } a, b, c \in R$$
3. There is a multiplicative identity denoted by 1_R with $1_R \neq 0_R$ such that $1_R \times_R a = a \times_R 1_R = a$ for all $a \in R$.

4. The operation $\times_R$ is distributive over $+_R$, that is,

$$(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$$

$$a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$$

Note: We do not worry about the inverse of $\times_R$.

2.1 Examples

1. $(\mathbb{Z}, +, \cdot)$:

   - $(\mathbb{Z}, +)$: abelian group
     (a) Associativity: $a + (b + c) = (a + b) + c$
     (b) Identity Element: $a + 0 = a = 0 + a$ (0 is the identity element)
     (c) Inverse: $a + (-a) = 0 = (-a) + a$
     (d) Abelian Property: $a + b = b + a$ for all $a, b \in \mathbb{Z}$
   - $(\mathbb{Z}, \cdot)$:
   - Distributive property: $a \cdot 1 = 1 \cdot a = a$, where 1 is the identity element.
   - Distributive property: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   - Distributive property: $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

2. $(\mathbb{R}, +_R, \times_R)$: $a \times_R b = b \times_R a$ for all $a, b \in \mathbb{R}$, hence it is a commutative ring.

3. $(\mathbb{Z}, +, \cdot)$: Commutative ring.

2.2 Units

An element a of a ring R is called a unit or an invertible element if there exists an element $b \in R$ such that $a \times_R b = 1_R$. (1 is the unit element in $(\mathbb{Z}, +, \cdot)$). The set of units in a ring R forms a group under the multiplication operation. This is known as the group of units of R. (Since, the inverse was missing and we added that as well).

3 Field

A field is a non-empty set F together with two binary operations, addition $(+)$ and multiplication $(\cdot)$, for which the following properties are satisfied:

1. $(F, +)$ is an abelian group.

2. If 0_F denotes the additive identity element of $(F, +)$, then $(F - \{0_F\}, \cdot)$ is an abelian group.

3. For all $a, b, c \in F$, we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

3.1 Examples

1. $(\mathbb{Z}, +, \cdot)$:
   - $(\mathbb{Z}, +)$ is an abelian group with identity element 0.
   - But for the set $\mathbb{Z} - \{0\}$, multiplicative inverse does not exist. Hence, $(\mathbb{Z} - \{0\}, \cdot)$ is not an abelian group.
   - Hence, $(\mathbb{Z}, +, \cdot)$ is not a field.
2. $(\mathbb{Q}, +, \cdot)$:
   - $(\mathbb{Z}, +)$ is an abelian group with identity element 0.
   - For the set $\mathbb{Q} - \{0\}$, multiplicative inverse exists for every rational number.
   - Multiplication is distributive over addition on rational numbers. Hence, $(\mathbb{Q}, +, \cdot)$ is a field.
3. $(\mathbb{F}_p, +_p, \cdot_p)$, where $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ and p is any prime number:
   - $+_p$: $(x + y) \mod p$ - Trivially, this is an abelian group.
   - $\cdot_p$: $(x \cdot y) \mod p$ - Remove 0 from $\mathbb{F}_p$ then $\gcd(x, p) = 1$ since p is prime. Also, it is trivial that $\cdot_p$ is distributive over $+_p$.
   - Hence $(\mathbb{F}_p, +_p, \cdot_p)$ is a field.

3.2 Field Extension

Suppose K_2 is a field with addition $(+)$ and multiplication $(\cdot)$. Suppose $K_1 \subseteq K_2$ is closed under both these operations such that K_1 itself is a field with the restriction of $+$ and $\cdot$ to the set K_1. Then K_1 is called a subfield of K_2 and K_2 is called a field extension of K_1.

4 Polynomial Ring

Let $(F, +, *)$ be a field. The set of polynomials of any degree $F[x]$ is defined as:

$$F[x] = \{a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots | a_i \in F\}$$

The polynomial ring, denoted as $F[x]$, consists of all polynomials in the variable x whose coefficients are elements of the field F. This ring is formed by combining the set of polynomials with the field's binary operations, thereby establishing a structure where polynomial addition and multiplication satisfy the ring properties.

$$(F[x], +, *) \rightarrow \text{Polynomial Ring}$$

Let $P_1(x) \in F[x] = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$

$P_2(x) \in F[x] = b_0 + b_1 \cdot x + \ldots + b_n \cdot x^n$

If we want to add the two polynomials:

$$P_1(x) + P_2(x) = (a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n) + (b_0 + b_1 \cdot x + \ldots + b_n \cdot x^n)$$

$$P_1(x) + P_2(x) = (a_0 + b_0) + (a_1 + b_1) \cdot x + \ldots + (a_n + b_n) \cdot x^n$$

Multiplication operation of the two polynomials:

$$P_1(x) * P_2(x) = (a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n) * (b_0 + b_1 \cdot x + \ldots + b_n \cdot x^n)$$

$$P_1(x) * P_2(x) = (a_0 * b_0) + (a_0 * b_1 + b_0 * a_1) \cdot x + \ldots + (a_n * b_n) \cdot x^n$$

Additive inverse of $P(x)$:

$$P(x) = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$$

$$P(-x) = -a_0 + (-a_1) \cdot x + \ldots + (-a_n) \cdot x^n$$

Clearly, $P(-x)$ is the additive inverse of $P(x)$. Here, the negative sign does not mean the standard negation.

A polynomial ring is formally defined as the set of all polynomials $F[x]$ along with the operations of addition $(+)$ and multiplication $(*)$, and it is referred to as a ring if it satisfies the following conditions:

1. $(F[x], +)$ is an abelian group.
2. $*$ is associative over $F[x]$.
3. An identity element over multiplication exists.
4. $*$ is distributive over $+$.

4.1 Example

Consider the set $F = \{0, 1\}$ and the field $(F, +_2, *_2)$. Therefore, the polynomial set $F_2[x]$ is:

$$F_2[x] = \{a_0 + a_1 \cdot x + \ldots | a_i \in F\}$$

Let us take two example polynomials:

$$p(x) = x + 1$$

$$q(x) = x^2 + x + 1$$

$$p(x) +_2 q(x) = (x + 1) +_2 (x^2 + x + 1) = x^2 + (1 +_2 1) \cdot x + (1 +_2 1) = x^2$$

$$p(x) *_2 q(x) = (x + 1) *_2 (x^2 + x + 1)$$

$$p(x) *_2 q(x) = (x^3 + x^2 + x) + (x^2 + x + 1) = x^3 + (1 +_2 1) \cdot x^2 + (1 +_2 1) \cdot x + 1$$

$$p(x) *_2 q(x) = x^3 + 1$$

Here, to get the coefficient of x^i, we will perform addition (of terms forming power i) or multiplication (of terms forming power i) modulo 2 operation.

5 Irreducible Polynomials

A polynomial $P(x) \in F[x]$ of degree $n \geq 1$ is called irreducible if it cannot be written in the form of $P_1(x) * P_2(x)$ with $P_1(x), P_2(x) \in F[x]$ and the degree of $P_1(x), P_2(x)$ must be greater than or equal to 1.

5.1 Important Property

$x^2 + 1$ belongs to $F_2[x]$.

$$(x + 1) * (x + 1) = x^2 + (1 + 1) * x + 1 = x^2 + 1.$$

Therefore, $x^2 + 1 = (x + 1) * (x + 1)$ in $F_2[x]$. Hence, $x^2 + 1$ is reducible in $F_2[x]$. Now, consider a set denoted by I, containing polynomials defined as:

$$I = \langle P(x) \rangle = \{q(x) * P(x) | q(x) \in F[x]\}$$

Also, consider the set denoted by $F[x]/\langle P(x) \rangle$, where each element is formed by dividing an element from $F[x]$ by $P(x)$.

For any $q(x) \in F[x]$, there exist polynomials $d(x)$ and $r(x)$ such that:

$$q(x) = d(x) * P(x) + r(x)$$

where $r(x) \in F[x]/\langle P(x) \rangle$.

Also, if $P(x)$ is an irreducible polynomial, then $(F[x]/\langle P(x) \rangle, +, *)$ forms a field. In this context, addition and multiplication operations are performed modulo $P(x)$. Notably, the degree of $r(x)$ is always less than the degree of $P(x)$.

5.2 Examples

1. $x^2 + 1$ in $\mathbb{R}[x]$:
   - It is not possible to factor $x^2 + 1$ in $\mathbb{R}[x]$, where $\mathbb{R}$ is the set of real numbers.
   - Let $P(x) = q_1(x) \cdot q_2(x)$.
   - $\text{Deg}(q_1) \geq 1$
   - $\text{Deg}(q_2) \geq 1$
   - $x^2 + 1 = 0$
   - $x^2 = -1$
   - $x = \pm i$
   - $(x + \alpha)$ and $(x - \alpha)$
   - It is not a reducible polynomial because to reduce, it would result in $(x + i)$ and $(x - i)$ which are complex numbers, but it is in $\mathbb{R}$ (Real numbers). So, it is irreducible.
2. $x^2 + x + 1$ in $\mathbb{F}_2[x]$, where $\mathbb{F}_2 = \{0, 1\}$:
   - The polynomial $P(x) = x^2 + x + 1$ is irreducible.
   - We will put $x = 0$ and $x = 1$:
   - $P(0) = 1$
   - $P(1) = 1$
   - So, $(x + 0)$ and $(x + 1)$ are not factors of $P(x)$. There are no degree 1 factors of this $P(x)$. Hence, it is irreducible.

Consider the set $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$: For any polynomial $q(x)$, we can express it as:

$$q(x) = d(x) \cdot P(x) + r(x)$$

where $\deg(d(x)) < 2$ and $\deg(r(x)) < 2$. The possible remainders $r(x)$ can be $\{0, 1, x, x+1\}$. If $P(x)$ is an n-degree polynomial under modulo 2, then there will be 2^{2n} polynomials in $r(x)$, meaning $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$ will have $2^2 = 4^2 = 16$ polynomials.

6 Primitive Polynomials

Consider the set $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$. We've established that if $P(x)$ is irreducible, then $(\mathbb{F}_2[x]/\langle x\rangle, +, *)$ forms a field. Now, suppose α is a root of $x^2+x+1=0$, i.e., $\alpha^2+\alpha+1=0$. This implies $\alpha^2 = -\alpha-1 = \alpha+1$. If α can generate all possible polynomials in $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$, then x^2+x+1 is termed a primitive polynomial.

Let's demonstrate this:

$$\langle\alpha\rangle = \{0, 1 = \alpha^0, \alpha, \alpha+1 = \alpha^2\}$$

The order of α, denoted as $O(\alpha)$, is 2. Hence, x^2+x+1 is a primitive polynomial.

6.1 Example

Consider $\mathbb{F}_2[x]/\langle x^3+x+1\rangle$. The maximum number of polynomials that can be generated: $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

Let's check if the root of $x^3+x+1=0$ is a generator:

$$\alpha^3+\alpha+1 = 0 \Rightarrow \alpha^3 = \alpha+1$$

$$\langle\alpha\rangle = \{0, 1 = \alpha^0, \alpha, \alpha^2, \alpha+1 = \alpha^3, \alpha^2+\alpha = \alpha^4, \alpha^2+\alpha+1 = \alpha^5, \alpha^2+1 = \alpha^6\}$$

Since we can generate all the polynomials, x^3+x+1 is a primitive polynomial.

Note that there may exist a polynomial that is not primitive but still forms a field. That implies we can find a multiplicative inverse. Consider the polynomial αx. Instead of $1/\alpha x$, we have the polynomial α^2+1/x^2+1, which results in 1 on multiplication.

$$x \cdot (x^2+1) = x^3+x = x+1+x = 1$$

Similarly, for x^2, the multiplicative inverse is x^2+x+1.

$$x^2 \cdot (x^2+x+1) = x^4+x^3+x^2 = x\cdot(x+1)+(x+1)+x^2$$

$$x^2 \cdot (x^2+x+1) = x^2+x+x+1+x^2 = 1$$

7 AES (Advanced Encryption Standard)

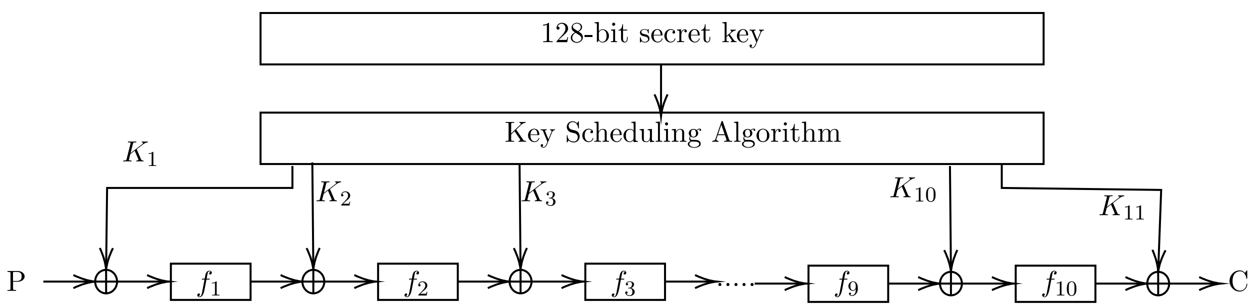
After DES was found to be vulnerable once it was released to the public, a new competition was held named AES to find a better cipher. In the competition, Rindel was the winning cipher and hence according to the rules of the competition, it was renamed to AES. AES is a NIST Standardized iterated block cipher and a substitution permutation network (SPN) as well.

Let us see the variations of AES:

1. **AES-128**:
    - Block size – 128 bit
    - Number of rounds – 10
    - Secret Key size – 128
2. **AES-192**:
    - Block size – 128 bit
    - Number of rounds – 12
    - Secret Key size – 192
3. **AES-256**:
    - Block size – 128 bit
    - Number of rounds – 14
    - Secret Key size – 256

Note: In all these three, only the number of rounds and the secret key size change!

7.1 Structure of AES



Important Observations -

- 10 Rounds
- 11 Keys Generated
- Ciphertext also of 128 bits