[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Aniruddh Modi (202151022) — Lecture 6 7 (Week 4)

1 Lecture 6

1.1 Groups

1.1.1 Subgroup of a group

A non-empty subset H of a group $(G, *)$ is a **subgroup** of G if H itself is a group on same symbol $*$. If H is alss a proper subset of G, then H is called a proper subgroup of G.

1.1.1.1 Example : Let $G = (Z, +)$ then $H = (0, +)$ is a subgroup.

1.1.2 Power operation in subgroup

If $(G, *)$ is a group, then $\forall a \in G$,

$$a^i = a * a * .... * a * a * a \in G$$

Proof of $a^i \in G$,

We now $\forall a \in G, a * a \in G$. Now let $b = a * a$. Since $b \in G, b * a \in G$. But we know that $b = a * a$. Hence, $\implies a * a * a \in G$

1.1.3 Cyclic group

If $\exists\ \alpha \in G$, such that $\forall b \in G$, there is an integer i with $b = \alpha^i$, then that group is called cyclic group and the element α is called the **generator** of $(G, *)$,

1.1.4 Order of an element

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 $(G, *)$

If G is finite, then all elements of G will have a finite order.

1.1.4.1 Example : Let $G = (Z_5, +_5)$. Then we can say that $O(0) = 1$, $O(1) = 5, O(2) = 5, O(3) = 5$ and $O(4) = 5$

Suppose some G has an element a such that $O(a) = 5$ Let $S = \{e, a, a^2, a^3, a^4\}$. Now, S is a cyclic subgroup.

If G is a group and $a \in G$, then set of all powers of a will form a cyclic subgroup denoted by $< a >$. (Even if G is infinite set, and for some $a \in G$, $O(a) = \infty$, even then $\{e, a, a^2, ...\}$ is also cyclic.

Also, $| < a > | = O(a)$ is true.

1.1.5 Lagrange's theorem

If G is a finite group and H is a subgroup if G then $|H| divides |G|$.

Let $a \in G$ and $O(a) = x$.

$$S = \{e, a, a^2, ..., a^{x-1}\} =< a >$$

Hence, S is a subgroup of G. Then $|S|$ divides $|G|$.

If the order of $a \in G$ is t, then order of a^k will be $\frac{t}{gcd(t,k)}$.

1.2 Ring

A ring $(R, +_r, \times_r)$ consists of a 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 identity element 0_r.
2. The operation $\times_r$ is associative.
3. There exists a multiplicative identity 1_r such that $1_r \neq 0_r$.
4. $\times_r$ is distributive over $+_r$.

$$(b +_r c) \times_r a = (b \times_r a) +_r (c \times_r a).$$

1.2.0.1 Example : $(Z, +, \cdot)$ is a ring.

1. $(Z, +) is an abelian group$
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. 1 is the multiplicative identity.
4. $\cdot$ is distributive over $+$.

1.2.1 Abelian ring

If $a \times_r b = b \times_r a$ is true $\forall a, b \in R$, then R is an abelian ring.

1.2.2 Invertible element

If there exits an element b such that $a \times_r b = 1_r$, then a is called invertible.

1.2.3 Groups of units

Set of all units forms a group under the $\times_r$ operator. This set if called group of units of R.

1.3 Fields

A field is a non empty set F together with two operators $+$ (additive) and $*$ (multiplicative) satisfying the following :

1. $(F, +)$ is an abelian group.
2. If 0_F denotes the additive identity then $(F \setminus \{0\}, *)$ is also an abelian group.
3. $\forall a, b, c \in F$, we have $a * (b + c) = (a * b) + (a * c)$

1.3.0.1 Example : $(Q, +, \cdot)$ is a field.

1.3.0.2 Example : $(Z, +, \cdot)$ is **not** a field.

1.3.0.3 Example : Let $\mathbb{F}_p = \{0, 1, 2, ..., p-1\}$ be a set where p is a prime number. Then,

$$(\mathbb{F}_p, +_p, \cdot_p) \text{ is a field}$$

1.3.1 Field Extension and sub-fields

Let K_2 be a field under $+$ and $*$ and $K_1 \subseteq K_2$. If K_1 itself is closed under both of these operators (operating with them will result in member of same set) and K_1 is also a field for the same operators, then K_1 is called the sub-field of K_2 and K_2 is called an extension of K_1.

2 Lecture 7

2.1 Polynomial Ring

Suppose $(\mathbb{F}, +, *)$ is field. Then $\mathbb{F}[x]$ is called a polynomial ring.

$$\mathbb{F}[x] = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n \mid a_i \in \mathbb{F}\}$$

2.1.1 Operations on $\mathbb{F}[x]$

Let $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ and $q(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$ such that $p(x), q(x) \in \mathbb{F}[x]$

2.1.1.1 Addition

$$p(x) + q(x) = r_0 + r_1x + r_2x^2 + ... + r_kx^k \tag{1}$$

where $r_i = a_i + b_i$ and $k = max(m, n)$

2.1.1.2 Multiplication

$$p(x) \times q(x) = s_0 + s_1x + s_2x^2 + ... + s_lx^l$$

where $s_i = p_0q_i + p_1q_{i-1} + ... + p_iq_0$

2.1.1.3 Example Let $\mathbb{F}_2 = \{0, 1\}$ be a set and $(\mathbb{F}_2, +_2, \times_2)$ be a field.

Let $p(x) = x +_2 1$ and $q(x) = x^2 +_2 x +_2 1$. Then,

$$p(x) +_2 q(x) = (x^2 + 2x + 2) \mod 2 = x^2$$
$$p(x) \times_2 q(x)s = (x^3 + 2x^2 + 2x + 1) \mod 2 = x^3 + 1$$

2.1.2 Irreducible polynomial

A polynomial $p(x) \in \mathbb{F}[x]$ of degree $n \geq 1$ is called irreducible if it cannot be written in the form of $p_1(x) \times p_2(x)$ with $p_1(x), p_2(x)$ and degree of $p_1(x), p_2(x)$ must be ≥ 1.

2.1.3 Ideals

An ideal I in a ring R is a subset of R that satisfies the following two properties:

1. Closed under addition. If $a, b \in I$, then $a + b\ inI$
2. Closed under multiplication. If $a, b \in I$, then $a \times b\ inI$

We define $< P(x) >$ as an ideal generated by $P(x) \in \mathbb{F}[x]$. It is the set of all polynomials in $\mathbb{F}[x]$ that can be written as the product of $P(x)$ and $Q(x) \in \mathbb{F}[x]$

$$I =< P(x) >= \{Q(x)P(x) \mid Q(x) \in \mathbb{F}[x]\}$$

2.1.4 Polynomial modulo operation

Let $P(x)$ be a irreducible polynomial. Then, we define $\mathbb{F}[x] — < P(x) >$ as the set of all polynomials with degree less than n. Then, we can represent $Q(x) \in \mathbb{F}[x]$ in the following form.

$$Q(x) = D(x) \times P(x) + R(x)$$

$$R(x) \in \mathbb{F}[x]/ < P(x) >$$

$$(\mathbb{F}\ / < P(x) >, +_{P(x)}, \times_{P(x)}) \text{ is a field where operators are under modulo } P(x)$$

2.1.5 Primitive Polynomial

Let $\mathbb{F}_2$ be a binary field ($\mathbb{F}_2 = \{0, 1\}$) with addition and multiplication under modulo 2. Let $\mathbb{F}_2[x]$ be a polynomial ring. Then, we know that $P(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. We know that $P(x)$ is irreducible. Then for $Q(x) \in \mathbb{F}_2[x]/P(x)$, we know $Q(x) = D(x)P(x) + R(x)$ exists such that $R(x) \in \mathbb{F}_2[x]/P(x)$. Now, $def(R(x) \leq 2)$. Hence, $R(x) = \{0, 1, x, x + 1\}$. Now, let $P(x) = 0$ then, $x^2 = -(x + 1) \mod 2 = x + 1$. Now, for all $G(x) \in \mathbb{F}_2[x]$, to find corresponding $R(x)$, replace x^2 with $x + 1$.

2.1.5.1 Example :

Let $G(x) = x^3$.

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

Hence, $x^3 \mod P(x) = 1$

2.2 AES

Advanced Encryption Standard is an iterated block cipher based on substitution-permutation network.

- ASE-128
  1. Block Size = 128 bit
  2. Number of rounds = 10

3. Secret key = 128 bit

- ASE-192
    1. Block Size = 128 bit
    2. Number of rounds = 12
    3. Secret key = 192 bit
- ASE-256
    1. Block Size = 128 bit
    2. Number of rounds = 14
    3. Secret key = 256 bit

2.2.1 ASE-128