
[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Chitranshi Srivastava (202051055)

Winter 2022-2023
Lecture 8 and 9 (Week #5)

In the previous week, we started mathematical recall about groups, abelian groups and finite groups before moving ahead to AES.

1 Mathematics Recall

1.1 Generators and Cyclic Group

Consider a group $(G, *)$. Let $\alpha \in G$. The identity element α^0 belongs to G . Therefore,

$$\alpha^0 * \alpha = \alpha^1$$

$$\alpha^1 * \alpha = \alpha^2$$

$$\alpha^2 * \alpha = \alpha^3$$

Note: The $*$ here is not multiplication, it is a binary operation not necessarily multiplication. $\alpha^1, \alpha^2, \alpha^3$ and so on, are just notation of using the binary operation $*$ on same element.

Since, G is closed under $*$, any two elements belonging to G , will give the result in G on performing the binary operation $*$. Since $\alpha^0 \in G$ and $\alpha \in G$, therefore $\alpha^1 \in G$. Now, since $\alpha^1 \in G$, therefore $\alpha^2 \in G$, and so on. That means,

$$\alpha^0, \alpha^1, \alpha^2, \dots \in G$$

The set $\alpha^0, \alpha^1, \alpha^2, \dots$ is denoted by $\langle \alpha \rangle$. Also, $\langle \alpha \rangle \subseteq G$. α is called the generator of $(G, *)$ iff:

for any $b \in G \exists i \geq 0$ such that $b = \alpha^i$ and hence $G \subseteq \langle \alpha \rangle$.

We can conclude that $(G, *) = \langle \alpha \rangle$

A group is called a cyclic group if there is an element $\alpha \in G$, such that for every $b \in G$, there is an integer i with $b = \alpha^i$. In simple words, every element in G can be expressed as some exponent of α , then α is the generator of G .

1.1.1 Order of an element

Consider $(G, *)$ and $|G|$: finite. Let $a \in G$.

We already know that a^0 is identity. Now, the order of an element is the least positive integer m such that $a^m = e$.

$$o(a) = m \text{ such that } a^m = e$$

Since $a^m = e$, so $a^{m+1} = a$, $a^{m+2} = a^2$ and so on. So we define a set H such as:

$$H = \{a^0, a^1, a^2, \dots, a^{m-1}\}$$

We understand that

- $H \subseteq G$
- H is a group under $*$

1.2 Lagrange's Theorem

If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$. G is a finite group and $a \in G$. We know that

$$H = \{a^0, a^1, a^2, \dots, a^{o(a)-1}\}$$

and H is a subgroup of G . $|H| = o(a)$.

So, using Lagrange's theorem, we can conclude that

$$|H| \mid |G| \Rightarrow o(a) \mid |G|$$

1.3 Some Results

- If the order of $a \in G$ is t , then

$$o(a^k) = \frac{t}{\gcd(t, k)}$$

- If $\gcd(t, k) = 1$, then

$$\begin{aligned} o(a^k) &= t = o(a) \\ \Rightarrow |\langle a^k \rangle| &= |\langle a \rangle| \end{aligned}$$

Let $x \in \langle a^k \rangle$, then $x = (a^k)^i = a^{ki}$

Now ki is also some integer so $a^{ki} \in \langle a \rangle$.

So, $\langle a^k \rangle \subseteq \langle a \rangle$. But the number of elements in both the sets is same. So, $\langle a^k \rangle = \langle a \rangle$.

Hence, a^k is also the generator of $\langle a \rangle$.

Example:

$Z_{19}^* = \{x \mid \gcd(x, 19) = 1, 1 \leq x \leq 18\}$, where

$*_{19}$: multiplication modulo 19 and

$x *_{19} y = (x y) \bmod 19$

Find the generators of $(Z_{19}^*, *_{19})$.

Solution:

$x \in Z_{19}^*$

$S = \{x^0, x^1, \dots\}$

Now let us check.

$\langle 2 \rangle = \{1, 2, 4, 8, 16, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10\} = Z_{19}^*$

So, $o(2) = 18$.

Let us see for 2^2 : $\gcd(19, 2) \neq 1$, so 2^2 is not a generator.

$\gcd(18, 5) = 1$, so 2^5 is also a generator and so on.

1.4 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

- $(R, +_R)$ is an abelian (commutative) group with the identity element 0_R
- The operation \times_R is associative, i.e.,

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

- There is a multiplicative identity denoted by 1_R with $1_R \neq 0_R$ such that

$$1_R \times_R a = a \times_R 1_R = a \quad \forall a \in R$$

- The operation \times_R is distributive over $+_R$, i.e.,

$$(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a) \text{ and } a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c) \text{ and}$$

Example:

$(\mathbb{R}, +_R, \times_R)$: check it is a ring or not.

Solution:

$(\mathbb{R}, +_R)$ is a commutative group with identity element 0 and -x as inverse. Real number 1 is identity and multiplication is associative and distributive hence it is a ring.

1.4.1 Commutative Ring

If the second operation is commutative, i.e, $a \times_R b = b \times_R a$, then it is commutative ring.

Both $(\mathbb{R}, +_R, \times_R)$ and $(\mathbb{Z}, +, \cdot)$ are commutative rings.

Note: Under the second operation, it does not necessarily be a group. It is not guaranteed that a multiplicative inverse will always be present.

If such elements are present that have multiplicative inverse (like 1 in case of \mathbb{Z}), we call those elements as unit elements or invertible elements of the ring such that

$$a \times_R b = 1_R$$

Example:

$(\mathbb{Z}_n, +_n, *_n)$ is a ring?

Solution:

First operation forms an abelian group over \mathbb{Z}_n . For $*_n$, 0 is the identity and it is both associative and distributive. Hence it is a ring. For all x in \mathbb{Z}_n , if $\gcd(x, n)=1$, then x has multiplicative inverse and it is unit element.

Note: The set of units in a ring R form a group under multiplication operation. This is known as group of units of R.

1.5 Field

A field is a non-empty set F together with two binary operation $+$ (addition) and $*$ (multiplication) for which the following properties are satisfied

- $(F, +)$ is an abelian group
- If 0_F denotes the additive identity element of $(F, +)$ then $(F \setminus \{0_F\}, *)$ is a commutative/abelian group.
- $\forall a, b, c \in F$, we have,

$$a*(b+c) = (a*b) + (a*c)$$

Example:

$(Z_P, +_P, *_P)$ is a Field ? Here, P is a prime number.

Solution:

Under, $+_P$ it is always an abelian group with 0 as identity element. Under $*_P$ is always associative and distributive. For all $Z_P - 0$, there is always an inverse under $*_P$ because since P is prime, $\gcd(x, P) = 1$ always. So, $*_P$ forms a commutative group on $Z_P - 0$. Hence, it is a Field.

Note:

- $(Z, +, \cdot)$ is not a field because inverse does not exist
- $(Q, +, \cdot)$
 $(Q, +)$: abelian group
 0 : additive identity
 1 : multiplicative identity
 $(Q \setminus \{0\}, \cdot)$ forms an abelian group.
 Hence, it is a field.

Example: Is $(\mathbb{F}_p, +_p, *_p)$ a field, where p is a prime number?

Solution: We know that $(\mathbb{F}_p, +_p)$ an abelian group with identity element 0. Now, the set $\mathbb{F}_p - \{0\}$ has existing multiplicative inverse iff $\gcd(x, p) = 1$ for each $x \in \mathbb{F}_p - \{0\}$. Since, p is prime, $\gcd(x, p) = 1$ for all possible integers that x can take. Hence, $(\mathbb{F}_p, +_p, *_p)$ is a field.

2 Field Extension

Suppose K_2 is a field with addition($+$) and multiplication($*$).

Suppose K_1 is closed under both these operations such that K_1 itself is a field with the restriction of $+$ and $*$ 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 .

3 Polynomial Ring

Let $(F, +, *)$ be a field and the set of polynomials of any degree $F[x]$ be:

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

$F[x]$ is set of all polynomials in x with coefficients belonging to set F of the given field. The set of polynomials along with the binary operations of the field forms a ring and this ring is known as polynomial ring.

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

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

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

If we want to add the two polynomials,

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

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

The coefficients a_i, b_i belong to set F and the addition operation is the field addition of the field $(F, +, *)$. Since $(F, +, *)$ is a field, therefore, $(F, +)$ is an abelian group and addition on elements of F is closed. Therefore, $P_1(x) + P_2(x)$ is closed under addition because for any i , $(a_i + b_i) \in F$. Also, addition of polynomials is just coefficient-wise, hence, addition of polynomials will be associative because of field properties of coefficients. Similarly, the additive identity of field will be the additive identity of the polynomial in $F[x]$. Now, let's look at additive inverse of $P(x)$.

$$\begin{aligned} P(x) &= a_0 + a_1 \cdot x + \dots + a_n \cdot x^n \\ P(-x) &= -a_0 + (-a_1) \cdot x + \dots + (-a_n) \cdot x^n \end{aligned}$$

Clearly, $P(-x)$ is additive inverse of $P(x)$. Here, the negative sign does not mean the standard negation. It implies the additive inverse of a_i in the field F . Also,

$$P_1(x) + P_2(x) = P_2(x) + P_1(x)$$

Therefore, under addition the polynomial set $F[x]$ is an abelian group. Now, let's look at the multiplication operation of the two polynomials:

$$\begin{aligned} P_1(x) * P_2(x) &= (a_0 + a_1 \cdot x + \dots + a_n \cdot x^n) * (b_0 + b_1 \cdot x + \dots + b_n \cdot x^n) \\ P_1(x) * P_2(x) &= (a_0 * b_0) + (a_0 * b_1 + b_0 * a_1) \cdot x + \dots + (a_n * b_n) \cdot x^n \end{aligned}$$

The multiplication operation is field multiplication operation and hence is associative, distributive. Also, the multiplicative identity also exists for the polynomials in $F[x]$. Hence, $(F[x], +, *)$ is a polynomial ring.

Let us define a polynomial ring formally. A set of polynomials $F[x]$ along with the operation of addition(+) and multiplication(*) is called a ring if:

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

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

$$\mathbb{F}_2[x] = \{a_0 + a_1 \cdot x + \dots | a_i \in \mathbb{F}\}$$

Let us just take two polynomials from this set:

$$\begin{aligned} p(x) &= x + 1 \\ q(x) &= x^2 + x + 1 \\ p(x) +_2 q(x) &= (x + 1) +_2 (x^2 + x + 1) = x^2 + (1 +_2 1) \cdot x + (1 +_2 1) = x^2 \\ p(x) *_2 q(x) &= (x + 1) *_2 (x^2 + x + 1) \\ p(x) *_2 q(x) &= (x^3 + x^2 + x) + (x^2 + x + 1) = x^3 + (1 +_2 1) \cdot x^2 + (1 +_2 1) \cdot x + 1 \\ p(x) *_2 q(x) &= x^3 + 1 \end{aligned}$$

4 Irreducible Polynomial

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 degree of $P_1(x), P_2(x)$ must be greater than or equal to 1. It means that $P(x)$ is irreducible if it can not be factorised.

Example: $x^2 + 1 \in \mathbb{F}_2[x]$.

Solution: $(x + 1) * (x + 1) = x^2 + (1 + 1) \cdot x + 1 = x^2 + 1$. Therefore, $(x^2 + 1) = (x + 1) * (x + 1)$ in $\mathbb{F}_2[x]$. Hence, $(x^2 + 1)$ is reducible in $\mathbb{F}_2[x]$. Note that it is not possible to factor $x^2 + 1$ in $\mathbb{R}[x]$, where \mathbb{R} is set of real numbers.

4.1 Ideal Generated by $P(x)$

It is a set denoted by I which contains the polynomials given as:

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

Consider the set denoted by $F[x]/\langle P(x) \rangle$ whose each element is formed by taking an element from $F[x]$ and then dividing it by $P(x)$. That is,

$$\begin{aligned} q(x) \in F[x] &= d(x) * P(x) + r(x) \\ r(x) &\in F[x]/\langle P(x) \rangle \end{aligned}$$

The remainder obtained belongs to the set $F[x]/\langle P(x) \rangle$. Now, if $P(x)$ is irreducible polynomial, then $(F[x]/\langle P(x) \rangle, +, *)$ becomes a field. Here, the addition and multiplication operation are under modulo $P(x)$. The degree of $r(x)$ is always lesser than degree of $P(x)$.

Example: $x^2 + x + 1 \in F_2[x]$, $F_2 = \{0, 1\}$. $P(x) = x^2 + x + 1$ is irreducible. Consider the set $F_2[x]/\langle x^2 + x + 1 \rangle$:

$$\begin{aligned} q(x) &= d(x) \cdot P(x) + r(x) \\ \deg(r(x)) &< 2 \\ r(x) &= \{0, 1, x, x + 1\} \end{aligned}$$

If $P(x)$ is a n degree polynomial under modulo 2, then there will be 2^n polynomials in $r(x)$, that is, $F_2[x]/\langle x^2 + x + 1 \rangle$.

Consider now for example a polynomial $X^2 + 1 \in F_2[x]$. Let's find the remainder on dividing it by $P(x)$. For F_2 , the remainder can be found in an easy way. It can be done by replacing x^2 in dividend with the lesser degree part of divisor, that is, $(x + 1)$. Therefore,

$$\begin{aligned} x^2 + 1 &= q(x) * (x^2 + x + 1) + r(x) \\ r(x) &= x + 1 + 1 = x \end{aligned}$$

Let's take another example, say, $x^3 + 1$:

$$\begin{aligned} x^3 + 1 &= q(x) * (x^2 + x + 1) + r(x) \\ r(x) &= x \cdot x^2 + 1 = x \cdot (x + 1) + 1 \\ r(x) &= x^2 + x + 1 = x + 1 + x + 1 = 0 \end{aligned}$$

We saw that the remainder came out to be 0 and x . We can take other examples where the remainder will come out to be the remaining two polynomials, that are, 1 and $(x + 1)$.

5 Primitive Polynomial

Consider the set $F_2[x]/\langle x^2+x+1 \rangle$. We have discussed that if the $P(x)$ is irreducible then $(F[x]/\langle P(x) \rangle, +, *)$ becomes a field. Now, let's say if α is a root of $x^2 + x + 1 = 0$, that is,

$$\begin{aligned}\alpha^2 + \alpha + 1 &= 0 \\ \alpha^2 &= -\alpha + (-1) = \alpha + 1\end{aligned}$$

If α can generate all the possible polynomials in $F_2[x]/\langle x^2 + x + 1 \rangle$, then $x^2 + x + 1$ is known as primitive polynomial. Now, let's see:

$$\begin{aligned}\langle \alpha \rangle &= \{0, 1 = \alpha^0, \alpha, \alpha + 1 = \alpha^2\} \\ O(\alpha) &= 2\end{aligned}$$

Hence, $x^2 + x + 1$ is a Primitive Polynomial.

Example: $\mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

Solution: 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 root of $x^3 + x + 1 = 0$ is a generator or not.

$$\begin{aligned}\alpha^3 + \alpha + 1 &= 0 \implies \alpha^3 = \alpha + 1 \\ \langle \alpha \rangle &= \{0, 1 = \alpha^0, \alpha, \alpha^2, \alpha + 1 = \alpha^3, \alpha^2 + \alpha = \alpha^4, \alpha^2 + \alpha + 1 = \alpha^5, \alpha^2 + 1 = \alpha^6\}\end{aligned}$$

Since, we are able to generate all the polynomials, therefore $x^3 + x + 1$ is a primitive polynomial. Note that there may exist a polynomial that is not a primitive polynomial but is still a field. That means, we will be able to find multiplicative inverse. Let us consider for the polynomial x . Instead of $1/x$, we have a polynomial $x^2 + 1$, which will give 1 as result on multiplication.

$$x * (x^2 + 1) = x^3 + x = x + 1 + x = 1$$

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

$$\begin{aligned}x^2 * (x^2 + x + 1) &= x^4 + x^3 + x^2 = x * (x + 1) + (x + 1) + x^2 \\ x^2 * (x^2 + x + 1) &= x^2 + x + x + 1 + x^2 = 1\end{aligned}$$

6 Advanced Encryption Standard

When the design of DES was made public, it was immediately broken. Thereafter, NIST called for a competition named Advanced Encryption Standard. A lot of cryptographers around the world submitted their designs along with the implementation. One of the submission in the competition was *Rijndael*. It was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. In the proposal, it was mentioned that the winner will be renamed as Advanced Encryption Standard. AES is unbreakable till date.

Advanced encryption Standard is an iterated block cipher and is based on Substitution Permutation Network (SPN). There are three different variants of AES:

1. AES-128 (Block Size 128-bit, Number of Rounds = 10, Secret Key Size 128-bit)
2. AES-192 (Block Size 128-bit, Number of Rounds = 12, Secret Key Size 192-bit)
3. AES-256 (Block Size 128-bit, Number of Rounds = 14, Secret Key Size 256-bit)

6.1 AES 128

