[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2022-2023
Scribed by: Akshay (202051018) — Lecture (Week 5)

1 Generator

A group (G, $\star$) is closed under $\star$
Let's say, $\alpha \in G$
and, $\alpha^0, \alpha^1, \alpha^2, ... \in G$, ____ (1) where α^0 is identity
α^n is outcome of applying $\star$ b/w α^n and α

> For any $b \in G$ if $\exists\ i \geq 0$ s.t. $b = \alpha^i$
> then, α is called the generator of $(G, \star)$ ____ (2)
> Such groups are called cyclic group.

From (1), $< \alpha > \subseteq G$ ____ (3)
From (2), $G \subseteq < \alpha >$ ____ (4) From (3) and (4) $(G, \star) = < \alpha >$

2 Order

$(G, \star)$ $|G| : finite$ $a \in G$

> Orde of 'a' i.e. O(a) is the leasr postive integer m such that $a^m = e$ (identity)
> O(a) = m

$a^0 (= e), a^1, a^2, ...a^{m-1} \in G$
H = $\{a^0, a^1, a^2, ...a^{m-1}\}$, After a^{m-1} every element will repeat ($\because a^m = e$)

1. $H \subseteq G$
2. H is group under $\star$ (you can check verify with properties)
    - $a^i \star a^{m-i} = a^0 = e \implies$ invertible

H is a sub-group of G.

3 Lagrange's theorem

> If G is a finite group and H is a sub-group of G then $|H|$ divides $|G|$

$O(a)$ *divides* $|G|$ because O(a) is cardinality of cyclic **sub-group** of G

Another Result:

> For $a \in G$,
> $$O(a^k) = \frac{O(a)}{gcd(O(a),k)} = \frac{t}{gcd(t,k)}$$
> where, t = O(a)

If gcd(t,k) =1 then,
$O(a^k) = t = O(a)$
$| < a^k > | = | < a > |$
$\implies < a^k > = < a >$
Reasoning:
$x \in < a^k >$
$\implies x = (a^k)^i = a^{ki} = a^{(some\ integer\ only)} \in < a >$
$\implies < a^k >$ **is also a generator of same cyclic group.**
Result:

> If k is co-prime O(a) then a^k is the generator of same set which 'a' generates.

4 Illustration:

$\mathbb{Z}_{19}^* = \{x \mid gcd(x,19) = 1,\ 1 \leq x \leq 18\}$
$\star_{19}$: multiplication modulo 19.
$x \star_{19} y = (x.y) mod 19$
Find the generator of the group $(\mathbb{Z}_{19}^*, \star_{19})$ **:**
$x \in \mathbb{Z}_{19}^*$
S = $\{x^0, x^1, ...\}$
$< 2 >$ = {1,2,4,8,16,13,7,14,9,18,17,15,11,3,6,12,5,10} = $\mathbb{Z}_{19}^*$
So, 2 is a generator.   O(2) = 18
32 (=2^5) is also a generator of $\mathbb{Z}_{19}^*$ because gcd(5,O(2)) = gcd(5,18) = 1.

5 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 i.e., $a \times_R (b \times_R c) = (a \times_R b) \times_R c$ $\forall$ a,b,c $\in$ R
3. There is a multiplicative identity denoted by 1_R with $1_R \neq 0_R$ s.t. $1_R \times_R a = a \times_R 1_R = a\ \forall a \in R$
4. The operation $\times_R$ is distributive over $+_R$ i.e.,
   $(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$,
   $a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$

5.1 Examples:

5.2

$(Z, +, \cdot)$: Check - ring or not.
Ring ✓

5.3

$(R, +_R, \times_R)$: Is it a ring? Yes ✓
If $a \times_R b = b \times_R a \;\; \forall a, b \in R$
then $(R, +_R, \times_R)$ is a commutative ring

$\boxed{\text{Commutativity is meaningful w.r.t second operation in ring}}$

An element 'a' of a ring R is called unit or an invertible element if there is an element $b \in R$ s.t. $a \times_R b = 1_R$
The set of units in a ring R forms a group under multiplication operation. This is known as group of units of R.

6 Field

A Field is a non-empty set F together with two binary operation + (addition) and * (multiplication) 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$\setminus\{0_F\}, \star$) is a commutative/abelian group
3. $\forall a, b, c \in F$, we have:
   a*(b+c) = (a*b)+(a*c) (distributive)

Example:
$(Z_p, +_p, \star_p)$, $Z_p = \{0, 1, ..., p-1\}$, p: prime
Field ✓

6.1 Field Extension

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

F : field (F,+,*)

F[x] = $\{a_0 + a_1 x + a_2 x^2 + ...|a_i \in F\}$
F[x] is a set of all polynomials whose coefficients are from the field F. We can choose any field for our F[x]. If we choose $\mathbb{F}_p$ then the coefficients will be from 0 to p-1. If we choose R field then

coefficients will be real numbers.

Polynomial ring, (F[x], +, *)
If we club F[x] (defined already) with plus and multiply operator then it will become a ring, more specifically, a polynomial ring.

$P_1(x) \in F[x] \qquad P_1(x) = a_0 + a_1x + a_2x^2$
$P_2(x) \in F[x] \qquad P_2(x) = b_0 + b_1x + b_2x^2$
$P_1(x) + P_2(x) = (a_0 + a_1x + a_2x^2) + (b_0 + b_1x + b_2x^2) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$
$(a_i + b_i)$: Field addition
Additive identity: $0 + 0.x + 0.x^2$
Additive inverse: $-a_0 - a_1x - a_2x^2$

Under addition it is abelian group $\checkmark$
* is associative
1 is multiplicative identity
* is distributive over +
Ring $\checkmark$

6.2 Irreducible Polynomial

A polynomial $P(x) \in F[x]$ of degree n (n ≥ 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 ≥ 1

$$P(x) \neq P_1(x) * P_2(x)$$

Example:
$\boldsymbol{x^2 + 1 \in \mathbb{F}_2[x]}$
$(x + 1) * (x + 1) = x^2 + (1 + 1)x + 1 = x^2 + 1$ (Don't forget: operations are under modulo 2)
$\implies (x^2 + 1) = (x + 1) * (x + 1)$ in $\mathbb{F}_2[x]$
$\implies x^2 + 1$ is reducible in $\mathbb{F}_2[x]$

$$I =< P(x) >= \{q(x).P(x) \mid q(x) \in F(x)\}$$

I : ideal generated by P(x)

$$\boldsymbol{F[x]/ < P(x) >}$$

For every $q(x) \in F[x], \;\; r(x) \in F[x]/ < P(x) >$
where $r(x)$ is obtained as remainder by dividing $q(x)$ with $P(x)$
$q(x) = d(x) * P(x) + r(x)$

Note: $\boxed{\text{degree(r(x))} < \text{degree(P(x))}}$

A Result:

$\boxed{\text{If } P(x) \text{ is an irreducible polynomial then } (F[x]/<P(x)>, +, *) \text{ becomes a field.}}$

After each operation in this field, outcome is stored as remainder we get by dividing with $< P(x) >$

Example:
$x^2 + x + 1 \in \mathbb{F}_2[x], \qquad (F_2 = \{0, 1\})$
$P(x) = x^2 + x + 1$, which is irreducible
$q(x) = d(x).P(x) + r(x) \qquad (q(x) \in \mathbb{F}_2[x])$

$$\boldsymbol{\mathbb{F}_2[x]/ < x^2 + x + 1 >}$$

deg(r(x)) < 2
We can construct these polynomials: x, 1, $x + 1$, 0
$r(x) \in \{0, 1, x, x + 1\}$

An instance:

$$\begin{array}{r|l} & \quad 1 \\ \cline{2-2} x^2 + x + 1 & x^2 + 1 \\ & \underline{x^2 + x + 1} \\ & \qquad x \end{array}$$

★
Observation from programming point of view:

- We can take xor of coefficients of dividend with $x^2 + x + 1$ to get to the remainder
- Remainder can be achieved by replacing x^2 (higher degree term in dividend) with $x + 1$ (part of divisor excluding higher degree term)
  $(x + 1) + 1 = x$

Another instance for clarity:

$$\begin{array}{r|l} & \ x + \ \ 1 \\ \cline{2-2} x^2 + x + 1 & x^3 + \ \ 1 \\ & \underline{x^3 + x^2 + x} \\ & \underline{x^2 + \ \ x + 1} \\ & \underline{x^2 + \ \ x + 1} \\ & \qquad 0 \end{array}$$

Now, let's do it with our programming hacks:
Replacer : $x + 1$ (taken from divisor by excluding higher degree term)

$$x^3 + 1$$

$$= x.x^2 + 1$$

$$= x(x+1) + 1$$
$$= x^2 + x + 1$$
$$= (x+1) + x + 1 = 0$$

6.3 Primitive Polynomial

$$\mathbb{F}_2[x]/ < x^2 + x + 1 >$$

$x^2 + x + 1 = 0$
Let α is a root of $x^2 + x + 1 = 0$
So, $\alpha^2 + \alpha + 1 = 0$
$\implies \alpha^2 = \alpha + 1$ (-1 = 1 under mod 2)
$\{0, 1 = \alpha^0, \alpha^1, \alpha^2 = \alpha + 1\}$ $\quad$ $O(\alpha) = 2$
Since, α is generating all the elements of the field (all possible polynomials r(x)), so, polynomial $x^2 + x + 1$ is a primitive polynomial.

$$\mathbb{F}_2[x]/ < x^3 + x + 1 >$$

Maximum number of polynomials degree < 3: $2^3 = 8$
$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$
$\alpha^3 + \alpha + 1 = 0 \implies \alpha^3 = \alpha + 1$
$\{0, \alpha^0, \alpha, \alpha^2, \alpha + 1, \alpha^2 + \alpha, \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1\}$
primitive polynomial ✓

7 Advanced Encryption Standard (AES)

It is standardized by NIST
- Rijndael: Winner design of Advanced Encryption Standard competition.
- Winner of competition was named as AES.

AES :

- Iterated block cipher
- It is based on SPN

Variants of AES :-
AES-128 :

- Block size = 128 bit
- Number of rounds = 10
- Secret key size = 128 bit

AES-192 :

- Block size = 128 bit
- Number of rounds = 12
- Secret Key size = 192 bit

AES-256 :

- Block size = 128 bit
- Number of rounds = 14
- Secret Key size = 256 bit