[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Manas Jitendrakumar Ingle (202151086) — Lecture 1,2 (Week 4)

1 Subgroup

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

1. $H \subseteq G$ or not
2. H is itself a group with $*$

Property:
$(G, *)$ is a Group
$a \in G \rightarrow a * a \in G, a * a * a \in G$
$a * a = a^2, a * a * a = a^3 \in G$
$a^i = a * a * \ldots * a \in G, (a * a)^i \rightarrow i$ operations $*$

2 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,

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

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

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

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.

2.0.1 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 $a^m = e$.

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

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:

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

We understand that

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

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
  $a \in G$
  $O(a) \mid |G|$
  $\Rightarrow a \in G$

  $H = \{\ e = a^0, a^1, a^2, \dots, a^{O(a)-1}\}$
  H is a subgroup of G

  From Lagrange's theorem:
  $|H| \mid |G|$
  $\Rightarrow O(a) \mid |G|$

- If the order of $a \in G$ is t
  then $O(a^k) = \frac{t}{gcd(t,k)}$

- If $gcd(t,k) = 1$
  then $O(a^k) = t = O(a)$
  $\Rightarrow |< a^k >| = |< a >|$

  $x \in < a^k >$
  $\Rightarrow x = (a^k)^i = a^{ki} =< a >$

  $< a^k > \subseteq < a >$
  $< a^k > = < a >$
  $< a^k > \subseteq < a >$
  $\Rightarrow < a^k > = < a >$
  a^k is also a generator of $< a >$
  $< a^k > = < a >$ Subgroup generated by a
  $< a > = < a^k >$ Subgroup generated by a^k

3 Ring:

3.1 Introduction:

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,
   $a \times_R (b \times_R c)$
3. There is a multiplication identity denoted by 1_R with $1_R \neq 0_R$ such that

   - $1_R \times_R a = a \times_R 1_R = a \qquad \forall a \in R$
4. The operation $\times_R$ is distributive over $+_n$,i.e,
   $(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$
   $a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$

Field

A field is a non-empty set F together with two binary operation +(addition) and *(multiplication) fow 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,

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

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.

4 Field Extension

Suppose K_2 is a field with addition(+) and multiplication(*).
Suppose $K_1 K_2$ 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.

As K_1 is a subset of K_2. Let F be a field $(F, +, *)$. Consider the polynomial ring $F[x]$, which consists of all polynomials with coefficients in the field F:

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

The addition operation of two polynomials in $F[x]$:

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}) + (b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-1} x^{n-1})$$

results in:

$$(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_{n-1} + b_{n-1})x^{n-1}$$

where $a_i + b_i$ is the additive operation in the field F. The multiplication operation of two polynomials in $F[x]$:

$$(a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}) * (b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-1} x^{n-1})$$

results in:

$$(a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \ldots + (a_{n-1} b_{n-1})x^{2n-2}$$

5 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.

6 Advanced Encryption Standard:

- It is Standardized by NIST.
- Rijndael - winner of Advanced Encryption Standard Competition.
- Winner of the Competition was named AES.

AES is based on -

1. Iterative block cipher.
2. It is based on SPN.

6.1 Types of AES:

1. AES - 128
    (a) Block size = 128 bit
    (b) Number of Rounds = 10
    (c) Secret key size = 128 bit
2. AES - 192
    (a) Block size = 128 bit
    (b) Number of Rounds = 12
    (c) Secret key size = 192 bit
3. AES - 256
    (a) Block size = 128 bit
    (b) Number of Rounds = 14
    (c) Secret key size = 256 bit