Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 5a: Introduction to Cryptography Mathematics- Part-3

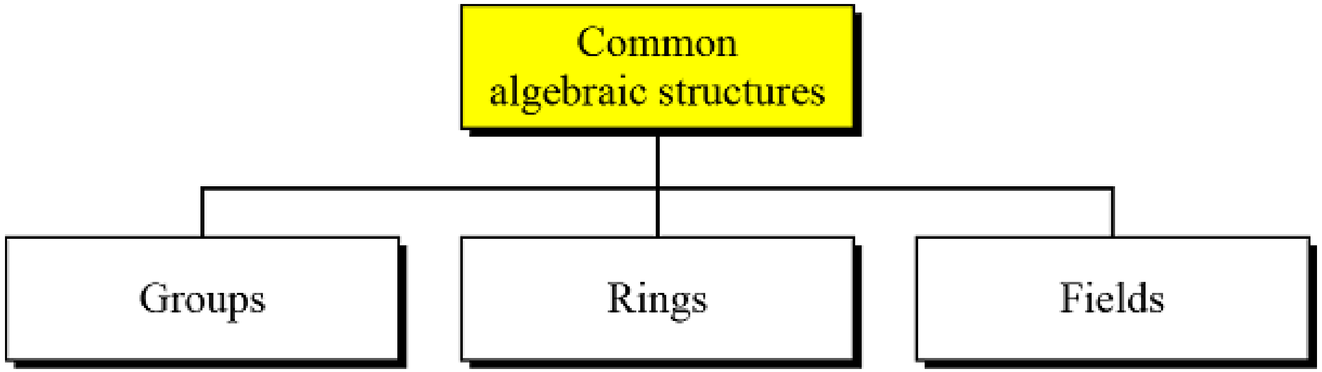
Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

ALGEBRAIC STRUCTURES

- Cryptography requires sets of integers and specific operations that are defined for those sets.
- The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.
- Three common algebraic structures:
  - Groups
  - Rings, and
  - Fields.



Groups

- A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms).
- Closure
  - If a and b are elements of G, then c = a•b is also an element of G.
- Associativity
  - If a, b and c are elements of G, then (a•b) •c=a•(b•c)
- Existence of identity
  - For all a in G, there exist an element e, called the identity element, such that e•a=a•e=a
- Existence of inverse
  - For each a in G, there exists an element a’, called the inverse of a, such that a•a’=a’•a=e

Groups

- A Commutative group (Abelian group) is group in which the operator satisfies four properties plus an extra property that is commutativity.
  - For all a and b in G, we have a • b = b • a
- Application
  - Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operations!!!!
- Example
  - *The set of residue integers with the addition operator,*
    $G = < Z_n , +>$,
    is a commutative group.
    Check the properties….

Groups

Let us check the properties.

1. Closure is satisfied. The result of adding two integers in Zn is another integer in Z_n.

2. Associativity is satisfied. The result of 4 + (3 + 2) is the same as (4 + 3) + 2.

3. Commutativity is satisfied. We have 3 + 5 = 5 + 3.

4. The identify element is 0. We have 3 + 0 = 0 + 3 = 3.

5. Every element has an additive inverse. The inverse of an element is its complement. For example, the inverse of 3 is −3 (n − 3 in Zn) and the inverse of−3 is 3. The inverse allows us to perform subtraction on the set.

Groups

- The set Z_n* with the multiplication operator, $G = \langle Z_n^*, \times \rangle$, is also an abelian group.
- We can perform multiplication and division on the elements of this set without moving out of the set.
- It is easy to check the first three properties.
- The identity element is 1.
- Each element has an inverse that can be found according to the extended Euclidean algorithm.

Groups

- Let us define a set G = < {a, b, c, d}, •> and the operation

•	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Check for properties….

- Is the group abelian????

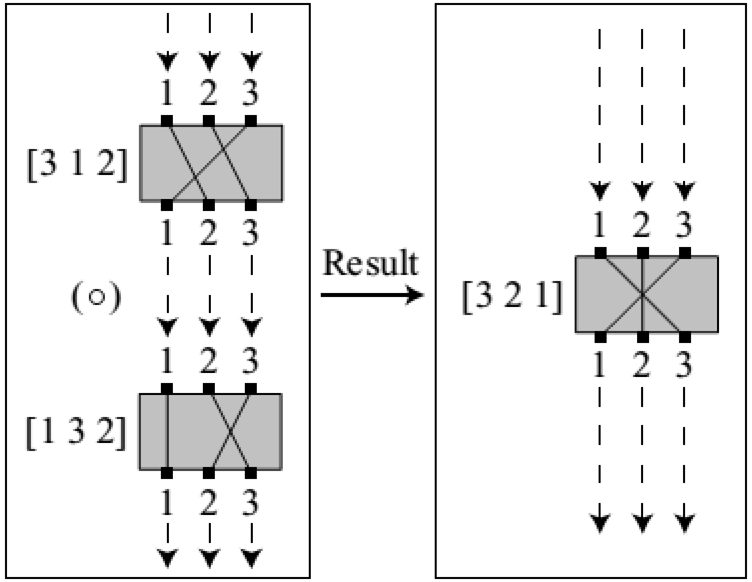
Groups

•	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

- This is an abelian group. All five properties are satisfied:
  1. Closure is satisfied. Applying the operation on any pair of elements result in another elements in the set.
  2. Associativity is also satisfied. To prove this we need to check the property for any combination of three elements. For example, (a + b) + c = a + (b + c) = d.
  3. The operation is commutative. We have a + b = b + a.
  4. The group has an identity element, which is a.
  5. Each element has an inverse. The inverse pairs can be found by finding the identity in each row (shaded). The pairs are (a, a), (b, d), (c, c).

Groups

- A very interesting group is the permutation group.
- The set is the set of all permutations, and the operation is composition: applying one permutation after another.



$\boxed{[3\ 2\ 1] = [3\ 1\ 2] \circ [1\ 3\ 2]}$

Read from right to left:
The first permutation is [1 3 2] followed by [3 1 2];
the result is [3 2 1].

Operation table for permutation group

∘	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

Check for properties….

- Is the group abelian????

Permutation group

- Closure is satisfied.
- Associativity is also satisfied.
- The commutative property is not satisfied.
- The set has an identity element, which is [1 2 3] (no permutation).
- Each element has an inverse.
- Set of permutations with the composition operation is a group.
- This implies that using two permutations one after another cannot strengthen the security of a cipher, because we can always find a permutation that can do the same job because of the closure property.

Groups

- Finite Group
  - If the set has a finite number of elements; otherwise, it is an infinite group.
- Order of a Group |G|
  - The number of elements in the group.
  - If the group is finite, its order is finite
- Subgroups
  - A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G
  - If G=<S, •> is a group, H=<T, •> is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G
  - If a and b are members of both groups, then c=a•b is also member of both groups
  - The group share the same identity element
  - If a is a member of both groups, the inverse of a is also a member of both groups
  - The group made of the identity element of G, H=<{e}, •>, is a subgroup of G
  - Each group is a subgroup of itself

Groups

- Finite Group
    - If the set has a finite number of elements; otherwise, it is an infinite group.
- Order of a Group |G|
    - The number of elements in the group.
    - If the group is finite, its order is finite
- Subgroups
    - A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G
    - If G=<S, •> is a group, H=<T, •> is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G
    - If a and b are members of both groups, then c=a•b is also member of both groups
    - The group share the same identity element
    - If a is a member of both groups, the inverse of a is also a member of both groups
    - The group made of the identity element of G, H=<{e}, •>, is a subgroup of G
    - Each group is a subgroup of itself

Groups

- Is the group $H = \langle Z_{10}, + \rangle$ a subgroup of the group $G = \langle Z_{12}, + \rangle$?
- The answer is no. Although H is a subset of G, the operations defined for these two groups are different. The operation in H is addition modulo 10; the operation in G is addition modulo 12.

Groups

- Cyclic subgroups
  - If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

$$\boxed{a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

Groups

- Four cyclic subgroups can be made from the group $G = <Z_6, +>$.
- They are $H_1 = <\{0\}, +>$, $H_2 = <\{0, 2, 4\}, +>$, $H_3 = <\{0, 3\}, +>$, and $H_4 = G$.

$0^0 \bmod 6 = 0$

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 +1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1+ 1) \bmod 6 = 5$

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

Groups

- Exercise:
  - Find out the cyclic subgroups for group $G = \langle Z_{10}*, \times \rangle$.

Groups

- Three cyclic subgroups can be made from the group G = <Z_{10}*, ×>.
- G has only four elements: 1, 3, 7, and 9.
- The cyclic subgroups are H_1 = <{1}, ×>, H_2 = <{1, 9}, ×>, and H_3 = G.

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

Groups

- Cyclic group
  – A cyclic group is a group that is its own cyclic subgroup.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

- Example:
  - Three cyclic subgroups can be made from the group G = <$Z_{10}*$, ×>.
  - The cyclic subgroups are H_1 = <{1}, ×>, H_2 = <{1, 9}, ×>, and H_3 = G.
  - The group G = <$Z_{10}*$, ×> is a cyclic group with two generators, g = 3 and g = 7.
  - The group G = <Z_6, +> is a cyclic group with two generators, g= 1 and g = 5.

Lagrange's Theorem

- Assume that G is a group, and H is a subgroup of G.
- If the order of G and H are |G| and |H|, respectively, then, based on this theorem, |H| divides |G| .
- Order of an Element
  – The order of an element is the order of the cyclic group it generates.
- Example:
  - In the group $G = <Z_6, +>$, the orders of the elements are:
    ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.
  - In the group $G = <Z_{10}^*, \times>$, the orders of the elements are:
    ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.