Chapter 4

Mathematis of cryptography

for moraler symmetric key cipher

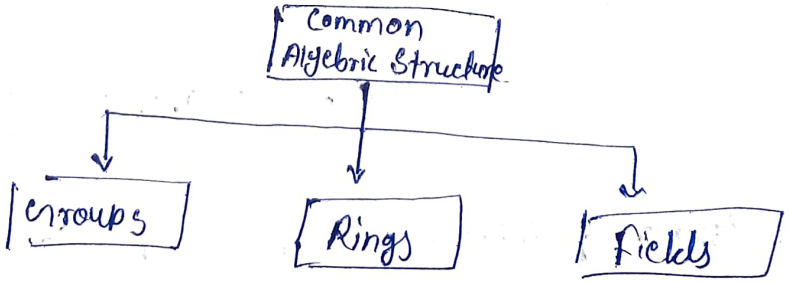
Algebraic Structure :-

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 algebric structure.

~~Example:~~ ~~Solution~~ *

there are three common algebric structures :-

1. Groups
2. Rings
3. Fields



Groups :-

denoted by $\{G, \cdot\}$

A group (G) is a set of elements with a binary operation '$\cdot$' that satisfies four properties. (CAIN)

(1) ~~Clous~~ Closure :- If a & b are the two elements of G then $c = a \cdot b$ is also an element of G.

$a, b \in G$ then $(a \cdot b) \in G$

(2) Associativity :- If a, b, c are elements of G, then

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$ for all $a, b, c \in G$

(3) Existence of identity :- for all 'a' in G there exists an element e called the identity element, such that

$$e \cdot a = a \cdot e = a$$ for all $a, e \in G$

(4) Existence of inverse :- for each 'a' in G there exists an element a' called the inverse of a such that

$$a \cdot a' = a' \cdot a = e$$

for all $a, a' \in G$

Abelian Group:- A group is said to be Abelian if it already a group and commutative property is also satisfied i.e $(a \cdot b) = (b \cdot a)$ for all a, b in G

Abelian Group :- Also called a commutative group, is a group in which the (•) operator satisfies the four properties. Plus an extra property 'commutativity'.

Commutativity :- for all a & b in G we have :

$$a \cdot b = b \cdot a \quad \text{for all } a, b \in G$$

NOTE :- A Group Support Both Addition/Substration or Multiplication/Division, But Not Both at the Same time.

Example $G = \langle \{a, b, c, d\}, \cdot \}$

Operation table for this

•	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 abelian group
Because all 5 property are satisfied

(1) Clouser satisfied; Because the result of operation is in that group.

(2) Associativity is also satisfied.

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

(3) Commutative :- $a+b = b+a = b$

(4) Identity :- 'a' is identity element

(5) Each element has inverse (a, a) (b, d) (d, b) (c, c)

Q Is $(Z,+)$ is a group

Sol^n

$Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

CAIN Property

Closure If $a=5$ $b=-2 \in Z$ then $(a+b)=-3 \in Z$ ✓

Associative $5+(3+7)=(5+3)+7 \in Z$ ✓

Identity $(5+0)=(0+5)=5$ for all $a \in Z$ ✓

Inverse $(5+-5)=(-5+5)=0$ fall $5, -5 \in Z$ ✓

Commutative $(5+9)=(9+5)$ for all $(9,5) \in Z$ ✓

So it is group and it also follow Commutative property so it is Abelian group also

Finite Group :- A group is called a finite group. If the set has a finite number of elements, otherwise it is an infinite group.

Order of Group :- The order of a group, $|G|$ is the number of elements in the group. If the group is not finite, its order is infinite. , If the group is finite, the order is finite.

Subgroup :- 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. satisfy all properties of group

In other words, If $G = \langle S, \circ \rangle$, $H = \langle T, \circ \rangle$ is a group under the same operation,

$\Rightarrow$ T is Non Empty Subset of S, then H is a subgroup of G.

from the above definition :-

1. If a & b are members of both groups, then $c = a \circ b$ is also member of both groups.
2. The group shares the same identity element.
3. If 'a' is member of both group then inverse of a is also a member of both groups.

④ The group made by identity element of G, that is $H = \langle \{e\}, \cdot \rangle$ is a subgroup of G.

⑤ Each group is a subgroup of itself

Example:- Is the group $H = \langle Z_{10}, + \rangle$ a subgroup of $G = \langle Z_{12}, + \rangle$?

Solution:- No,

H is a subset of G, But The operations Defined on the groups are different:

The operation in H is addition modulo 10,
The operation in G is addition modulo 12.

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

The term power here means reapeatedly applying the group operation to the element:

$$a^n \rightarrow a \cdot a \cdot a \cdots a \quad (n \text{ times})$$

The set made from this Proces is referred to as $\langle a \rangle$.

$$\boxed{a^0 = e}$$

Example :- Cyclic Group can be made from the group $G = \langle Z_6, + \rangle$ is

(1) $H_1 = \langle \{0\}, + \rangle$

$0^0 \bmod 6 = 0$

{ cyclic group generated from 0

(2) $H_2 = \langle \{0, 2, 4\}, + \rangle$

$2^0 \bmod 6 = 0$ $\because e = 0 = a^0$

$2^1 \bmod 6 = 2$

$2^2 \bmod 6 = 4$

$(2+2) \bmod 6$

{ cyclic group generated from 2

(3) $H_3 = \langle \{0, 3\}, + \rangle$

$3^0 \bmod 6 = 0$

$3^1 \bmod 6 = 3$

$3^2 \bmod 6 = 0$

$(3+3) \bmod 6$

{ cyclic group generated from 3

(4) $H_4 = \langle Z_6, + \rangle$

$1^0 \bmod 6 = 0$

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

$1^3 \bmod 6 = (1+1+1) \bmod 6 = 3$

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

$1^5 \bmod 6 = (1+1+1+1+1) \bmod 6 = 5$

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

$1^1 \bmod 6 = 1$

{ cyclic group generated from 1

Example :- A group $G = \langle Z_{10}^*, \times \rangle$ has only 4 elements $\{1, 3, 7, 9\}$

The cyclic subgroup that can be formed are :-

(1) The cyclic group generated from 1 is

$1^0 \bmod 10 = 1$
$1^1 \bmod 10 = 1$
$1^2 \bmod 10 = 1$

$= \boxed{H_1 = \langle \{1\}, \times \rangle}$

(2) The cyclic group generated from 3 is

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^4 \bmod 10 = 7$

$= \boxed{H_2 = \langle Z_{10}^*, \times \rangle}$ that is G itself.

(3) The cyclic subgroup generated from 7 is

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

$= \boxed{H_3 = \langle Z_{10}^*, \times \rangle}$ G Itself

(4) The cyclic subgroup generated from 9 is

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

$= \boxed{H_4 = \langle \{1, 9\}, \times \rangle}$

A group G denoted by $\{G, \cdot\}$ is said to be a cyclic group if it contains at-least one generator element

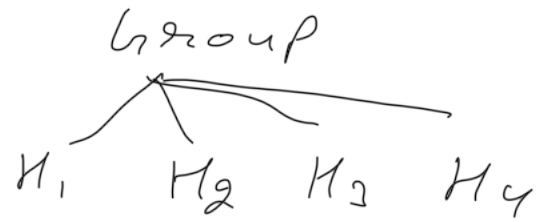
Subgroup

Let $(G, *)$ is a group (* → composition binary) then let $H \subset G$ is a non-empty subset of G

If $(H, *)$ satisfy the properties of group

1. Closure
2. Associative
3. Identity
4. Inverse

then we say that $(H, *)$ is a subgroup



$H_1 \cap H_2$ is a subgroup

Infinite intersection of subgroup is a group

$H_1 \cup H_2$ might not be subgroup

eg:- $(I, +)$ is a group

$H_1 = \{ 2x, x \in I \}$

$H_2 = \{ 3x, x \in I \}$

$\{-1, -4, -2, 0, 2, 4, \ldots\}$

$\{-9, -6, -3, 0, 3, 6, 9, \ldots\}$

$H_1 \cup H_2$

$\{-4, -3, -2, 0, 2, 3, 4, 6, 8, 9 \ldots\}$

Taking 2 and 3

$2 + 3 = 5 \notin H_1 \cup H_2$

so closure not hold

so $H_1 \cup H_2$ is not a subgroup

Cyclic Group :-

If there is an element 'g' of group 'G' which has a capability to generates all the elements of group 'G', then g is called generator of G. & G is called a cyclic group.

It can be written as

$\{e, g, g^2, \ldots g^{n-1}\}$ where $g^n = e = g^0$

NOTE :- A cyclic group can have many generator.

A group G denoted by $\{G, \cdot\}$ is said to be a cyclic group if it contains at-least one generator element

Example :-

(1) The group $G = \langle Z_6, + \rangle$ is a cyclic group with two generators $g=1$ & $g=5$

(2) The group $G = \langle Z_{10}^*, \times \rangle$ is a cyclic group with two generators $g=3$ & $g=7$

Langrange's theorem :- It relates the order of a group to order of its subgroup.

Assume that G is a group & H is a subgroup of G.

If order of G & H are $|G|$ & $|H|$ respectively, then based on this theorem $|H|$ divides $|G|$.

Q Prove that $(G, *)$ is a cyclic group where $G = \{1, \omega, \omega^2\}$

Soln

Composition Table

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Not a generator

$1^1 = 1$

$1^2 = 1 * 1 = 1$

$1^3 = 1 * 1 * 1 = 1$

$1^4 = 1 * 1 * 1 * 1 = 1$

$\omega^1 = \omega$

$\omega^2 = \omega * \omega = \omega^2$

$\omega^3 = \omega * \omega * \omega = \omega^3 = 1$

$\omega^4 = \omega * \omega * \omega * \omega = \omega^4 = \omega\omega^3 = \omega$

generator

$(\omega^2)^1 = \omega^2$

$(\omega^2)^2 = \omega^4 = \omega$

$(\omega^2)^3 = \omega^6 = 1$

$(\omega^2)^4 = \omega^8 = \omega^2$

generator

The generator of $(G, *)$ are ω and ω^2.

$(G, *)$ is a cyclic group

Q when does group G with operation '*' is said to be a cyclic group?

Sol^n

Let us take an element x

$G = \{ \ldots x^{-4}, x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, x^4 \ldots \}$

= Group generated by x

If $G = \langle x \rangle$ for some x then we call G a cyclic group

Q when does group G with operation '+' is said to be a cyclic group?

Sol^n

Let us take an element y

$G = \{ \ldots, -4y, -3y, -2y, -y, 0, y, 2y, 3y, 4y \ldots \}$

= Group generated by y

If $h = \langle y \rangle$ for some y, then we call G a cyclic group

Q A group $G \langle Z_6, + \rangle$ is cyclic group prove

Sol^n

$Z_6 = \{1, 2, 3, 4, 5\}$

$1^1 = 1 = 1$

$1^2 = 1+1 = 2$ generator

$1^3 = 1+1+1 = 3$

$1^4 = 1+1+1+1 = 4$

$1^5 = 1+1+1+1+1 = 5$

$2^1 = 2 = 2 \bmod 6 = 2$

$2^2 = 2+2 = 4 \bmod 6 = 4$ not a generator

$2^3 = 2+2+2 = 6 \bmod 6 = 0$

$2^4 = 2+2+2+2 = 8 \bmod 6 = 2$

$2^5 = 2+2+2+2+2 = 10 \bmod 6 = 4$

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

$3^2 = 3+3 = 6 \bmod 6 = 0$ not a generator

$3^3 = 3+3+3 = 9 \bmod 6 = 3$

$3^4 = 3+3+3+3 = 12 \bmod 6 = 0$

$3^5 = 3+3+3+3+3 = 15 \bmod 6 = 3$

$4^1 = 4 = 4 \bmod 6 = 4$

$4^2 = 4+4 = 8 \bmod 6 = 2$ not a generator

$4^3 = 4+4+4 = 12 \bmod 6 = 0$

$4^4 = 4+4+4+4 = 16 \bmod 6 = 4$

$4^5 = 4+4+4+4+4 = 20 \bmod 6 = 2$

$5^1 = 5 \bmod 6 = 5$

$5^2 = 5+5 = 10 \bmod 6 = 4$ generator

$5^3 = 5+5+5 = 15 \bmod 6 = 3$

$5^4 = 5+5+5+5 = 20 \bmod 6 = 2$

$5^5 = 5+5+5+5+5 = 25 \bmod 6 = 1$

The generator G $\langle Z_6, + \rangle$ is 1, 5

$\langle Z_6, + \rangle$ is a cyclic group

Q A group G $\langle Z_{10}^*, * \rangle$ is cyclic group prove it

$Z_{10}^* = \{1, 3, 7, 9\}$

$1^1 = 1$ not a generator

$1^2 = 1 * 1 = 1$

$1^3 = 1 * 1 * 1 = 1$

$3^1 = 3 \bmod 10 = 3$

$3^2 = 3 * 3 = 9 \bmod 10 = 9$ generator

$3^3 = 3 * 3 * 3 = 27 \bmod 10 = 7$

$3^4 = 3 * 3 * 3 * 3 = 81 \bmod 10 = 1$

$3^5 = 3 * 3 * 3 * 3 * 3 = 273 \bmod 10 = 3$

$7^1 = 7 \bmod 10 = 7$

$7^2 = 49 \bmod 10 = 9$

$7^3 = 343 \bmod 10 = 3$

$7^4 = 2401 \bmod 10 = 1$ generator

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

$9^2 = 81 \bmod 10 = 1$ not a generator

$9^3 = 729 \bmod 10 = 9$

$9^4 = 6561 \bmod 10 = 1$

generator of $\langle Z_{10}^*, * \rangle$ is 3, 7

$\langle Z_{10}^*, * \rangle$ is a cyclic group

Langrange's theorem

1) $f(x)$ is continuous in $[a,b]$ $\quad [f(a) \neq f(b)]$

2) $f(x)$ is Differentiable in (a,b)

then $x = c \in (a,b)$

$$f'(c) = \frac{f(b) - f(a)}{b-a}$$

eg:- $f(x) = x^2 - 4x - 3$

$a = 1 \quad b = 4$

soln

It is continuous

It is Differentiable

$f(a) \neq f(b)$

$f(1) = (1)^2 - 4(1) - 3 = -6$

$f(4) = (4)^2 - 4(4) - 3 = -3$

$$f'(c) = \frac{-3 - (-6)}{4-1} = 1$$

$c^2 - 4c - 3$

$2c - 4 = 1$

$2c = 5$

$c = \frac{5}{2} = 2.5 \in (1,4)$

For Example :- The order of the group $G = \langle Z_{17}, +_7 \rangle$ is 17, The only Divisor of 17 is 1 & 17

This means that this group has only two Subgroups, $H_1 = \langle \{0\}, + \rangle$ & $H_2 = G$ Itself.

 # Order of Element :- The order of Element is the order of cyclic group it generates.

Example :-

In the group $G = \langle Z_6, + \rangle$ the orders of the elements are :-

$ord(0) = 1$	$ord(2) = 3$	$ord(4) = 3$
$ord(1) = 6$	$ord(3) = 2$	$ord(5) = 6$

In the group $G = \langle Z_{10}^*, \times \rangle$ the order of the element are :-

$ord(1) = 1$, $ord(3) = 4$, $ord(7) = 4$, $ord(9) = 2$

Order of an element :- Let $(G, *)$ be a group order is defined for $\forall a \in G$

→ Denoted by $O(a)$

$O(a) = n$

where n is smallest positive integer which satisfy the eq^n $a^n = e$

→ Order of identity element is always 1

→ Order of an element and it's inverse is always same

→ Order of an element in an infinite group does't exist or infinite except identity

→ $O\{-1, 1, -i, i\}$ ✗

Q find order of element $O\{0,1,2,3\}, +_4$

$0^1 = 0$ $1^1 = 1$ $2^1 = 2$ $3^1 = 3$

$0^2 = 0$ $1^2 = 1+1 = 2$ $2^2 = 2+2 = 4$ $3^2 = 6 \Rightarrow 2$

$0^3 = 0$ $1^3 = 3$ $2^3 = 6 \Rightarrow 2$ $3^3 = 9 \Rightarrow 1$

$0^4 = 0$ $1^4 = 1+1+1+1$ $2^4 = 8 \Rightarrow 0$ $3^4 = 12 \Rightarrow 0$

$= 4 \bmod 4$

$= 0$

Note:- here we stop where we got our identity element

$O(0) = 1$ $O(2) = 4$

$O(1) = 4$ $O(3) = 4$

Ring :-

A Ring is denoted as $R = \langle \{ \ldots \}, \cdot, \square \rangle$ is an algebric structure with two operations.

The first operation must ~~sets~~ satisfy all five Properties required for an abelian group.

The second operation must satisfy only the first two. In addition, the second operation must be distributed over the first.

Distributivity means that for all $a, b, \& c$ element of R we have

$$a \square (b \cdot c) = (a \square b) \cdot (a \square c) \quad \&$$

$$(a \cdot b) \square c = (a \square c) \cdot (b \square c)$$

A Commutative Ring :- It is a Ring in which the commutative property is also satisfied for the second operation.

Example :- $R = \langle Z, +, \times \rangle$ is a commutative Ring.

Rings

A ring R denoted by $\{R, +, *\}$ is a set of elements with two binary operations called addition and multiplication, such that for all $a, b, c \in R$

Rings follow these properties :-

1. Group (A1-A4), Abelian Group
2. Closure under multiplication (M1)

   If $a, b \in R$ then $ab \in R$
3. Associativity of multiplication (M2)

   $a(bc) = (ab)c$ for all $a, b, c \in R$
4. Distributive Law (M3)

   $a(b+c) = ab + ac$ for all $a, b, c \in R$

   $(a+b)c = ac + bc$ for all $a, b, c \in R$

Note :-

Subtraction [$a - b = a + (-b)$]

Commutative Rings

A ring is said to be commutative, if it satisfies the following additional condition:

Commutativity of multiplication (M4)

$ab = ba$ for all $a, b \in R$

Integral Domain

An integral domain is a commutative ring that obeys the following axioms:

Multiplicative identity (M5): There is an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$

No zero divisors (M6) :- If $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$

Fields

A field F, sometimes denoted by $\{F, +, *\}$ is a set of elements with two binary operations called addition and multiplication, such that for all $a, b, c \in F$ the following axioms are obeyed

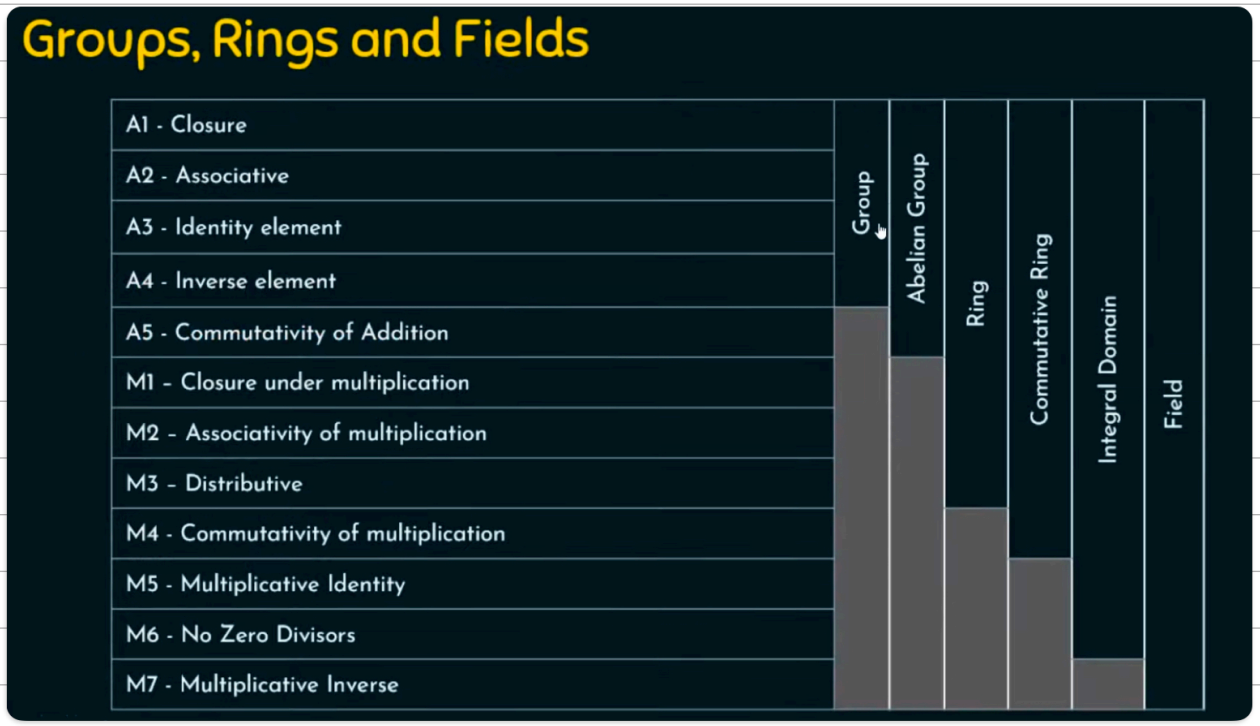
→ (A1-M6): F is an integral domain; that is F satisfies axioms A1-A5 and M1-M6

→ (M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that

$$aa^{-1} = (a^{-1})a = 1$$

Note = $a/b = a(b^{-1})$

eg:- Rational no
Real no
Complex no



Finite Fields

A finite field or Galois field is a field that contains a finite no of elements.

As with any field, a finite field is a set on which the operations of multiplication, addition, subtraction and division are defined and satisfy certain basic rules

the most common examples of finite fields are given by the integers (mod p) when p is a prime no.

Application areas :-

Mathmatics :- Number theory, Algebraic geometry, Galois theory finite geometry

field :- A field, denoted by $f = \langle \{..\}, \cdot, \square \rangle$ is a commutative Ring with the second operator ~~Property~~ ~~Define~~ satisfied by all the 5 operation.

except that the identity element of the first operation has no inverse with respect to the second operation.

finite field :- Also we have a infinite field But only finite fields extensively used in cryptography. A finite field a field with finite Number of elements, are very important structure in cryptography.

Galois field :- Galois showed that for a field to be finite, the number of element should be p^n, where p is prime & n is positive integer. The finite field usually called Galois field and denoted as $GF(p^n)$.

~~GF(p)~~ GF(p) fields :- When $n=1$, we have GF(p) field. This field can be the set $Z_p \{0, 1, \ldots p-1\}$ with two Arithmetic operations (addition & multiplication). Each element in this set has an additive inverse & that nonzero element have a multiplicative inverse. ~~except~~ except 0.

Ex:- A very common field in this category is $GF(2)$ with the set $\{0,1\}$ and two operation addition and Multiplication.

$$GF(2) = \langle \{0,1\}, +, \cdot \rangle$$

Addition =

+	0	1
0	0	1
1	1	0

Multiplication

·	0	1
0	0	0
1	0	1

Additive Inverse

a	0	1
$-a$	0	-1

Multiplicative Inverse

a	0	1
a^{-1}	X	1

IN this $GF(2)$:-

The addition operation work as 'XOR' & The Multiplicative operation work as 'AND'.

$GF(p^n)$ field :- In addition to $GF(p)$ fields, we are also interested in $GF(p^n)$ fields in cryptography.

However the set Z, Z_n, Z_n^*, Z_p, which we are used so far with operations such as addition and Multiplication, cannot satisfy the requirement of field. Some new ~~operation~~ Set & Some new Operations on those sets must be defined.

GF(2^n) Fields :- In cryptography we often need to use four operations (Addition, Substraction, Multiplication & Division). So we need to use fields.

When we work with computer, the positive integers are stored in computer as n bit words in which n is usually 8, 16, 32, 64 & so on. This means the range of integer is 0 to $2^n - 1$. The modulus is 2^n. So we have two choices if we want to use a field :-

(1) We can use GF(P) with the set Z_P, where P is the largest prime number less than 2^n. But this scheme is inefficient because we can not use the integers P to $2^n - 1$.

(2) We can work in GF(2^n) and uses a set of 2^n elements. The elements in this set are n-bit words.

Polynomials :-

Polynomials are useful when we have to perform addition & multiplication operation on n-bit word.

Although we can directly Define Rules for addition & multiplication operation on n-bit words. But It is easier when we represents a number or n-bit words In polynomial of digree n-1.

The n-bit word can be represented as :-

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} \cdots a_0 x^0$$

where x^i is ith bit
& a_i is coefficient → 0 If Bit is 0
→ 1 If Bit is 1

To Representing n-bit word as polynomial we have to follow some Rules :-

(1) The Power of x defines the position of ith Bit. x^{n-1} is left most bit
x^0 is Rightmost bit.

(2) The coefficients of the terms defins the value of the bits. Because a bit can have only a value 0 or 1, so our polynomial coefficients can be either 0 or 1.

Example:- How to represent 8-bit word (10011001) using a polynomials.

n bit word 1 0 0 1 1 0 0 1

Polynomial $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

first Simplification $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification $x^7 + x^4 + x^3 + 1$

#Operations:- Any Polynomial Actually involves two operations :-

→ Operation on cofficients
→ operation on two Polynomials.

In other words, we need to define two fields, one for coefficients and on for Polynomials.

Cofficient are made of 0 & 1, So we can use $GF(2)$ field for this purpose.

for the Polynomials we need the field $GF(2^n)$

NOTE:- Polynomials representing n-bit words using two fields : $GF(2)$ and $GF(2^n)$

Modulus :-

Now we have to know about this facts before performing any operations on polynomials:

(1) Addition of two polynomials never creates a Polynomial out of the set.

(2) Multiplication of two polynomials may creates a polynomial with digree more then n-1.

This means we need to divide the result by a modulus & keep only a remainder.

(3) Modulus in this case ~~~~ is a

Prime Polynomial.

which means it can not be factorized in the polynomial of digree less then n.

Such polynomial also called irreducible Polynomials.

(4) For each digree we can have more then one irreducible polynomials.

List of irreducible polynomials of degree ~~then~~ 1 to 5.

Degree	Irreducible Polynomial
1	$(x+1), (x)$
2	$(x^2+x+1), (x^2+1)$
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+1), (x^4+x+1)$
5	$(x^5+x^2+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1)$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

Addition:-

Addition is very easy, Because the addition of 2 polynomial do not creates a polynomial of degree more then n-1. So we do not need to reduce it.

Ex:- $(x^5+x^2+x) \oplus (x^3+x^2+1)$ in $GF(2^8)$

$$\begin{array}{r} 0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \\ + \quad 0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \\ \hline 0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 \end{array}$$

$\Rightarrow \boxed{x^5 + x^3 + x + 1}$

Additive inverse :- The additive Inverse of a Polynomial with coefficients in Gf(2) is polynomial itself.

Additive Identity :- The additive identity in a Polynomial is a zero Polynomial.

Multiplication :- Multiplication in Polynomials is the sum of the multiplication of each term of the first polynomial with each term in second polynomial.

we need to remember 3 Points :-

(1) The cofficient multiplication is done in Gf(2)

(2) Multiplying x^i by x^j result in $x^{(i+j)}$

(3) Multiplication may create terms with digree more then n-1., which means the result needs to reduced using a modulus polynomials.

find the result of

$(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible Polynomial $x^8 + x^4 + x^3 + x + 1$.

here $\otimes$ is multiplication of two polynomials.

Solve

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$

$$= x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$

$$= x^{12} + x^7 + x^2$$

Now we have to reduce this using irreduseble polynomial $x^8 + x^4 + x^3 + x + 1$

$$x^8 + x^4 + x^3 + x + 1 \;\Big|\; x^{12} + x^7 + x^2$$

$x^4 + 1$

$x^{12} + x^7 + x^2$

$x^{12} + x^8 + x^7 + x^5 + x^4$

$x^8 + x^5 + x^4 + x^2$

$x^8 + x^4 + x^3 + x + 1$

Remainder $\boxed{x^5 + x^3 + x^2 + x + 1}$ Ans

Multiplicative Identity :- The multiplicative identity is always 1. for example in $GF(2^8)$ the multiplicative inverse is 00000001

Multiplicative Inverse :- We can find Multiplicative inverse using extended Euclidean algorithm.

Ex:-

In $GF(2^4)$ find the inverse of (x^2+1) modulo (x^4+x+1)

q	r_1	r_2	r	t_1	t_2	t
x^2+1	(x^4+x+1)	(x^2+1)	x	0	1	x^2+1
x	x^2+1	x	1	1	x^2+1	x^3+x+1
x	x	1	0	x^2+1	x^3+x+1	1
	1	0		x^3+x+1	0	

Find the multiplicative inverse

x^5 modulo $(x^8+x^4+x^3+x+1)$

q	r_1	r_2	r	t_1	t_2	t
x^3	$x^8+x^4+x^3+x+1$	x^5	x^4+x^3+x+1	0	1	x^3
$x+1$	x^5	x^4+x^3+x+1	x^3+x^2+1	1	x^3	x^4+x^3+1
x	x^4+x^3+x+1	x^3+x^2+1	1	x^3	x^4+x^3+1	$x^5+x^4+x^3+x$
x^3+x^2+1	x^3+x^2+1	1	0	x^4+x^3+1	$x^5+x^4+x^3+x$	0
	1	0		$(x^5+x^4+x^3+x)$	0	

↑ Ans

$x^5 \overline{)\, x^8+x^4+x^3+x+1 \,(\, x^3}$

x^8

x^4+x^3+x+1

$x^4+x^3+x+1 \overline{)\, x^5 \,(\, x+1}$

$x^5+x^4+x^2+x$

x^4+x^2+x

x^4+x^3+x+1

x^3+x^2+1

$x^3+x^2+1 \overline{)\, x^4+x^3+x+1 \,(\, x$

x^4+x^3+x+1

1

$(x^4+x^3+1)+(x^3+x^2+1)$

$x^5+x^4+x^3+x$

$\Rightarrow x^4+x^3+1+x^8+x^7+x^6+x^4+x^7+x^6+x^5+x^3+x^5+x^4+x^3+x$

$= x^8+x^4+x^3+x+1$

$= (x^8+x^4+x^3+x+1) \mod (x^8+x^4+x^3+x+1)$

$= 0$