Mathematics of Symmetric key Cryptography:-

Symmetric Encryption:-

- Symmetric Ciphers use symmetric algorithms to encrypt and decrypt data
- These ciphers are used in symmetric key Cryptography.
- A symmetric algorithm uses the same key to encrypt data as it does to decrypt data.

Example:

A symetric algorithm will use key k to encrypt some plaintext information like a password into a Ciphertext.

Then it uses k again to take the Ciphertext and turn it back into the password.

- Symmetric Ciphers are opposite of asymmetric ciphers, like those used in public-key-cryptography.
- Ciphers use asymmetric algorithm which use one key to encrypt data and a different key to decrypt ciphers.
- These, two keys are called public and private keys as to the case with RSA encryption.
- The public key is used to encrypt data and private key is used to decrypt data.

M. ANBARASU. M.Sc., M.S., (SSE)., M.Tech., (CSE)., PhD.,

Explain the network security model with neat sketch?

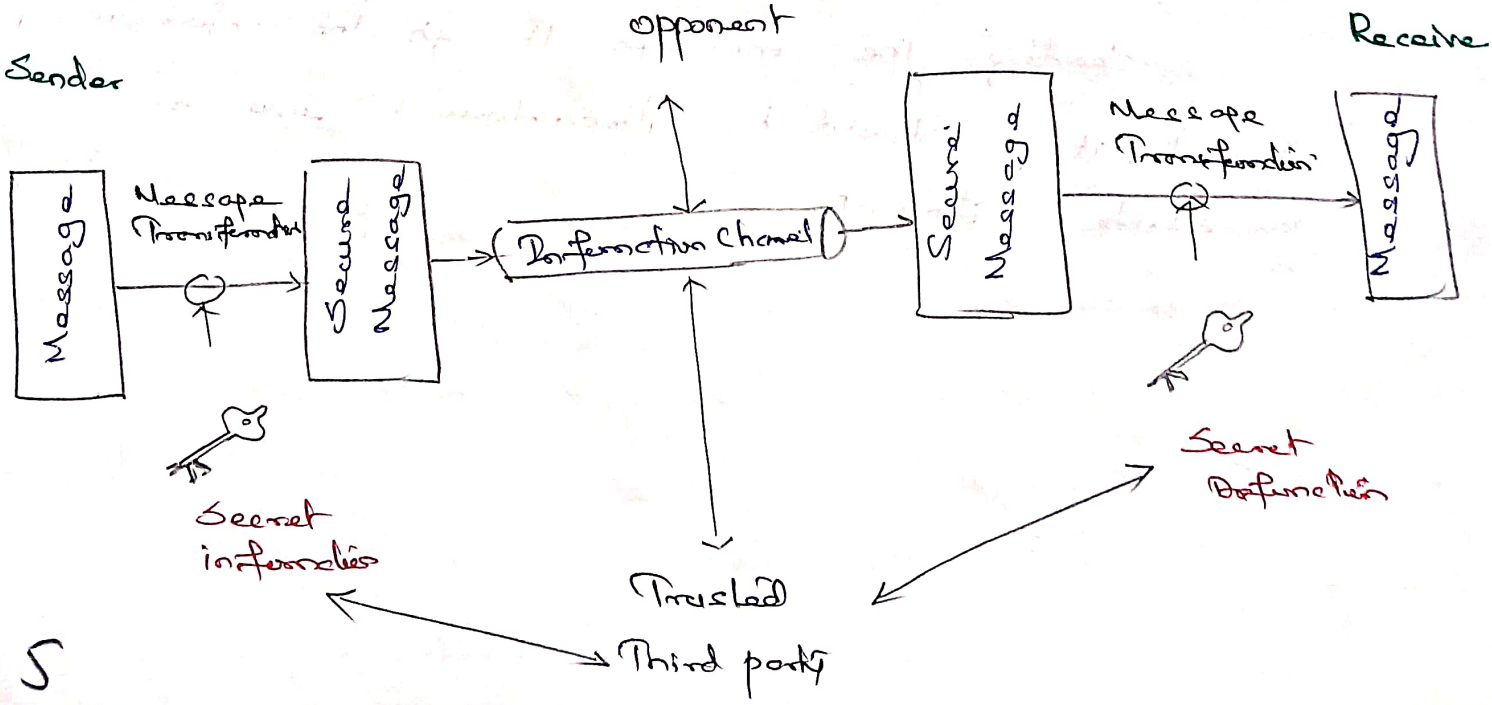
N/w Security Model with neat sketch:

N/w security Model exhibits how the security service has been designed over the n/w to prevent the opponent from causing a threat to the Confidentiality or authenticity of the information that is being transmitted through the n/w.

1. Transformation of the information which has to be sent to the receiver. So that any opponent present at the intermediate channel is unable to read the message.

This indicates the encryption of the message.

It includes the additional code along the transformation of the information, which will be used in verifying the identity of the authentic receiver.



2. Secret information: b/w sender and the receiver of the which the opponent must not any else.

The encryption key which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. Trusted third party: which should take the responsibility of distributing the secret information (key) to both the communicating parties and also prevent it from any opponents.

→ The n/w security model print the two communicating parties Sender and receiver who mutually agrees to exchange information

→ But sender cannot send the message on the information channel in the readable form as it will have a threat being attacked by the opponent.

→ Sending the message through the information channel, it should be transformed into an unreadable format.

Introduction to Symmetric Cryptography:

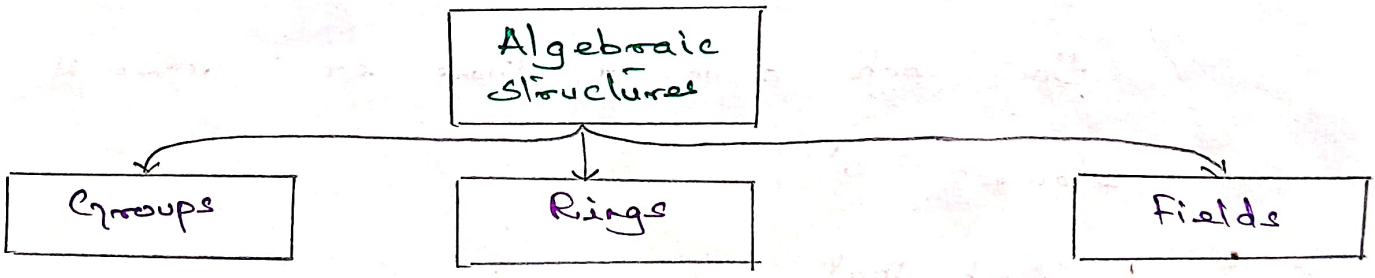
Mathematics of Symmetric Key Cryptography:-

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 element of the set is called an algebraic structures.

1. Groups
2. Rings
3. Fields are the fundamental elements of branch of Mathematics knows as abstract algebra (or) modern algebra.



Groups:

A group G, denoted by $\{G, *\}$ is a set of elements with a binary operation denoted by $\cdot$ that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G,

such that the following axioms are satisfied.

(i) Closure:

if a and b are elements of G,

then

$$a \cdot b \in G$$

(ii) Associative:-

if a, b and c are elements of G,

then

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall \quad a, b, c \in G$$

(iii) Identity :

For all a in G, there exists an element e, called the identity element, such that

$$a \cdot e = e \cdot a = a \quad \forall \quad a \in G$$

(iv) Inverse:-

For each a in G, there exist inverse of a, an element a',

such that

$$a \cdot a' = a' \cdot a = e \quad \forall a \in G$$

Satisfies the above (i), (ii), (iii) and (iv) is known it as a group.

If a group has a finite no: of element called a finite group and the order of the group is equal to the no: of elements in the group, otherwise the group is an infinite group.

Abelian Group :-

A group 'G' is said to be abelian, if it satisfies one additional property, that is commutative.

$$a \cdot b = b \cdot a \quad \forall \quad a, b \in G$$

Note :-

Abelian group is also called Commutative group.

ie :- Abelian group has following.

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

} Group

5. Commutative

} Abelian group

Cyclic Group :-

Defn: A group G is said to be cyclic if an element $a \in G$, such that every element of G can be expressed as a power of a.

for multiplicative group :

$$G = \{ x = a^n / n \in z \}$$

for Additive group :-

$$G = \{ x = na / n \in z \}$$

Note :- 'a' is called a Generator of G,

$$G = \langle a \rangle$$

GCD: (Greatest Common Divisor)

A gcd (a, b) of a and b is the largest number that divides evenly into both a and b.

Ex: GCD (60, 24) = ?

$$2 \mid 60 \quad 2 \mid 30 \quad 3 \mid 15 \quad 5$$

$$2 \mid 24 \quad 3 \mid 12 \quad 2 \mid 4 \quad 2$$

60 : $2 \times 2 \times 3 \times 5$
24 : $2 \times 2 \times 3 \times 2$

} Common divisor is $2 \times 2 \times 3 = 12$

GCD (60, 24) is 12

Ex:- GCD (8, 15) = ?

$$2 \mid 8 \quad 2 \mid 4 \quad 2$$

$$3 \mid 15 \quad 5$$

8 : $2 \times 2 \times 2$
15 : 3×5

} Common divisor is NIL

No Common factors

Note:- 1 is also consider as a common factor for GCD. but it is common for all elements.

Lagrenge's Theorem:-

A group G, and H is a subgroups of G.

If the order of G and H are |G| and |H| respectively,

Then $\frac{O(G)}{O(H)}$ =

Rings:-

A ring denoted as R, (R, *, □) is an algebraic structure with two binary operations *, □.

The (*) must satisfy all five properties of the abelian group:

1. closure
2. associative
3. identity
4. inverse
5. commutative

The (□) must satisfy only these two properties

1. closure
2. associative

Also the second operation (□) must be distributive over the first operation (*)

6. Distributive

Distributive: for all a, b and c elements of R,

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

and

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

A ring in which the Commutative property is also satisfied for the second operation is called a Commutative ring.

Ring with Unity:-

A ring R is said to be a ring unity, if the multiplicative identity.

$$1 \in R$$

such that

$$\boxed{1 \cdot a = a \cdot 1 = a} \quad \forall \; a \in R$$

Commutative Ring:-

A ring R is said to be a Commutative ring,

if

$$\boxed{a \cdot b = b \cdot a} \quad \forall \; a, b \in R$$

Ex:-

* Set of integers

  $Z = \{ \ldots -2, -1, 0, 1, 2, \ldots \}$ under the addition and multiplication is a Commutative ring with unity.

* Set of all natural numbers:

  $N = \{1, 2, 3 \ldots\}$ is not a ring.

* Set $E = \{ \ldots -4, -2, 0, 2, 4, \ldots \}$ of all even integers is a Commutative ring without unit element.

Field:-

A field F, denoted by $F = \langle \{\dots 3, *, \square\} \rangle$ is a commutative ring in which the second operation satisfies all five properties defined for the first operations, except that the identity element of the first operation + has no inverse with respect to the second operation.

The finite field is a field with, finite number of elements.

Galois showed that for a field to be finite, the number of elements should be p^n, where p is prime and n is positive integer.

The finite fields are usually called Galois field and denoted as $GF(p^n)$.

A Galois field, $\boxed{GF(p^n)}$ is a finite field with p^n elements.

GF(P) Fields:

When $n = 1$, we have GF(p) field.

$Z_p = \{0, 1, 2, \dots, p-1\}$ is a GF(p) field with two operations

$\boxed{\text{Addition Modulo } p}$

and

$\boxed{\text{Multiplication Modulo } p}$

Example:-

Z_7 is a GF(p) field with two operations: addition Modulo 7 and Multiplication Modulo 7.

Here we are defining GF(7) or Z_7 with two operations.

additive inverse

w	w^{-1}
0	0
1	6
2	5
3	4
4	3
5	2
6	1

+ (a \ b)	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	2
4	4	5	6	10	11	12	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Addition Modulo 7

identity element = 0

$(a+b) \bmod 7$.

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

multiplicative inverse

w	-w	w^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Additive and Multiplicative Inverse of Modulo 7

X	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication Modulo 7

identity element = 1

GF(2^n) is show no: of elements in FINITE FIELD of prime P^n

Justification :-

Galois Field (GF):

In GF, we need to perform

+, −, * and ÷,

so we need something that qualifies for a field.

* Z_p qualifies to be a field.
* In this view Z_n domain dealing with bits.

Ex:-

(i) Domain ⇒ Z_8 $2^3 = 8$

bits ⇒ 3

(ii) Domain ⇒ Z_{256} $2^8 = 256$

bits ⇒ 8

* Even integers domain are all above.
* Z_{256} and Z_8 are Commutative Rings.

Finite field of prime number GF(P^n)

$n = 1 \Rightarrow GF(P^1) \Rightarrow GF(P)$

$n > 1 \Rightarrow \ldots \Rightarrow GF(P^n)$

* GF(P) = set of Z_p integers $\{0, 1, 2, \ldots, n-1\}$

Eg: GF(2) : $F = \langle Z_p, +, * \rangle$

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

a	−a	a^{-1}
0	0	-
1	1	1

$GF(2^n) \equiv GF(P^n)$

$GF(2^3)$

Frequency of elements is evenly distributed in Addition

$2^2 2^1 2^0$

+	000	001	010	011	100	101	110	111
000	0	1	2	3	4	5	6	7
001	1	0	3	2	5	4	7	6
010	2	3	0	1	6	7	4	5
011	3	2	1	0	7	6	5	4
100	4	5	6	7	0	1	2	3
101	5	4	7	6	1	0	3	2
110	6	7	4	5	2	3	0	1
111	7	6	5	4	3	2	1	0

XOR
001
011
010
$2 \leftarrow 2^0 2^1 2^0$

← XOR

Do XOR
011
100
111
$7 = 4+2+1 \leftarrow 2^2 2^1 2^0$

2 XOR
110
110
000

a	-a	a^{-1}
0	0	-
1	1	1
2	5	5
3	3	6
4	4	7
5	5	2
6	6	3
7		

*	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	1	2	3	4	5	6	7
010	0	2	4	6	3	1	7	5
011	0	3	6	5	7	4	1	2
100	0	4	3	7	6	2	5	1
101	0	5	1	4	2	7	3	6
110	0	6	7	1	5	3	2	4
111	0	7	5	2	1	6	4	3

Modular Polynomial Arithmetic :-

GF(2^n) order of polynomial will never exceed $n-1$. If some operations it exceeds $n-1$ then perform mod order n irreducible polynomial.

1	0	0	1	0	1	0	1
x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0

This can be written as

$$x^7 + x^4 + x^2 + x^0$$

$$\Rightarrow \boxed{x^7 + x^4 + x^2 + 1}.$$

1	0	1	0	1	1	0	1
x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0

This can be written as:

$$x^7 + x^5 + x^3 + x^2 + x^0$$

$$\Rightarrow \boxed{x^7 + x^5 + x^3 + x^2 + 1}$$

For GF(2^n) order of polynomial will never exceed $n-1$.

If, after some operation, the order exceeds $n-1$, then perform mod order n irreducible polynomial.

000	001	010	011	100	101	110	111
$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$	$x^2x^1x^0$
0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

Division:-

Qn: $f(x) = x^3+x^2+2$ $\quad g(x) = x^2-x+1$

$x+2$ ← quotient

x^2-x+1 | x^3+x^2+2

$-x^3+x^2-x$

$2x^2-x+2$

$2x^2-2x+2$

x ← Remainder.

divisor

Qn: $f(x) = 4x^3+2x+3$ $\quad g(x) = 2x^2+x+1$

$2x$

$2x^2+x+1$ | $4x^3+2x+3$

$4x^3+2x^2+2x$

$-2x^2+3$

Qn: $f(x) = x^4+2x^2+x+5$ $\quad g(x) = x^2+x+1$

x^2+x+2 ← quotient.

x^2+x+1 | x^4+2x^2+x+5

$x^4+x^3+x^2$

$-x^3+x^2+x+5$

x^3+x^2+x

$2x^2+2x+5$

$2x^2+2x+2$

Remainder is 3

divisor

Q:- What are the generators of the Cyclic group $(Z_8, +)$?

Solution:-

The elements of Z_8 is 0, 1, 2, 3, 4, 5, 6, 7

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

To find the generators,

$\gcd(0, 8) = 8$
$\gcd(1, 8) = 1$
$\gcd(2, 8) = 2$
$\gcd(3, 8) = 1$
$\gcd(4, 8) = 4$
$\gcd(5, 8) = 1$
$\gcd(6, 8) = 2$
$\gcd(7, 8) = 1$

Finally the generators are 1, 3, 5 and 7. Under addition

Polynomials:-

Ordinary Polynomial Arithmetic:-

Let $f(x) = x^3 + x^2 + 2$
$g(x) = x^2 - x + 1$

Addition:

$f(x) + g(x) = x^3 + x^2 + 2 + (x^2 - x + 1)$
$= \boxed{x^3 + 2x^2 - x + 3}$

Multiplication:

$f(x) \times g(x) = (x^3 + x^2 + 2)(x^2 - x + 1)$
$= x^5 - x^4 + x^3 + x^4 - x^3 + x^2 + 2x^2 - 2x - 2$
$= \boxed{x^5 + 3x^2 - 2x - 2}$

Subtraction:-

$f(x) - g(x) = x^3 + x^2 + 2 - x^2 + x - 1 = \boxed{x^3 + x + 1}$.

ANBARASU.M, M.Sc., M.S (SS)., M.Tech (CSE)., Ph.D., Associate Professor., TEC

Polynomial arithmetic with Modulo Coefficients :-

→ All coefficients are 0 (or) 1.

→ It is a polynomial ring.

→ We are went to do in mod 2.

Ex:- **Addition :-**

Let $f(x) = x^3 + x^2$

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

			x^3	x^2	x^1	x^0	
$f(x)$	$= x^3 + x^2$	$\Rightarrow$	1	1	0	0	
$g(x)$	$= x^2 + x + 1$	$\Rightarrow$	0	1	1	1	+
			1	0	1	1	← XOR

Result :

$$f(x) + g(x) = x^3 + x^0 + 1$$

Multiplication :-

$f(x) = x^3 + x^2$ $\Rightarrow$ 1 1 0 0

$g(x) = x^2 + x + 1$ $\Rightarrow$ 0 1 1 1

1 1 0 0 X 0 1 1 1

1 1 0 0

1 1 0 0

1 1 0 0

0 0 0 0

0 1 0 0 1 0 0

x^6 x^5 x^4 x^3 x^2 x^1 x^0

$f(x) \times g(x) = 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 0x^1 + 0x^0$

$$f(x) \times g(x) = x^5 + x^2$$

Qn: Find the 8-bit word related to the polynomial x^6+x^3+x

x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
0	1	0	0	1	0	1	0

This is related to the 8-bit word 01001010

Note:- Polynomial representing n-bit words use two fields:
GF(2) and GF(2^n)

Qn: Figure show how we can represent the 8-bit word (10011001) using a polynomial?

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 $1x^7+1x^4+1x^3+1x^0$ $\boxed{x^0=1}$

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

Points:-

* A prime polynomial cannot be factored into a polynomial with degree of less than n. Such polynomials are referred to as Irreducible polynomials.

Ex:

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

} Irreducible polynomials.

Encryption:-

```
00110101   Plain Text
11100011   Secret key.
--------
11010110   Cipher Text.
```

XOR

Decryption:-

```
11010110   Cipher Text
11100011   Secret key.
--------
00110101   plain Text.
```

The addition in GF(2) means the exclusive-or (XOR) operation. So we can exclusive-or the two words, bits by bits. To get the result.

In the example:-

$x^5 + x^2 + x$ is 00100110

$x^3 + x^2 + 1$ is 00001101

Result is:- 00101011

The polynomial notation: $x^5 + x^3 + x + 1$

Qn:- Let us define a $GF(2^2)$ field in which the set has four 2-bit word.

$\{00, 01, 10, 11\}$

We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied.

$GF(2^2) = \langle \{00, 01, 10, 11\}, \oplus, \otimes \rangle$

Addition:-

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$$\begin{array}{r} 10 \\ \oplus\ 00 \\ \hline 10 \end{array} \qquad \begin{array}{r} 10 \\ \oplus\ 01 \\ \hline 11 \end{array} \qquad \begin{array}{r} 10 \\ \oplus\ 10 \\ \hline 00 \end{array} \qquad \begin{array}{r} 10 \\ \oplus\ 11 \\ \hline 01 \end{array}$$

Multiplication:-

$\otimes$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01

$0x^1 + 1x^0$

The set is $\{00, 01, 10, 11\}$

Corresponding polynomial are:-

$0x^1+0x^1$	$1x^1+0x^0$ / $1x^1+1x^0$	
00	01	10
0	1	x	$x+1$

Q1. Generate the elements of the field $GF(2^4)$ using the irreducible polynomial $f(x) = x^4 + x + 1$.

The elements $0, g^0, g^1, g^2$ and g^3 can be easily generated, because they are the first most of $0, 1, x^2, x^3$

$0 = 0\ 0\ 0\ 0$
$g^0 = 0\ 0\ 0\ 1$
$g^1 = 0\ 0\ 1\ 0$
$g^2 = 0\ 1\ 0\ 0$
$g^3 = 1\ 0\ 0\ 0$

$g^3\ g^2\ g^1\ g^0$