UNIT-I

17-12-2024

What is Cryptography?

Cryptography is used to secure and protect data during communication. It is helpful to prevent unauthorized person or group of users from accessing any confidential data.

Encryption and decryption are the two essential functionalities of Cryptography.

Meant By Encryption:?

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message.

That's why a hacker is not able to read the data as senders use as encryption algorithm. Encryption is usually done using key algorithms.

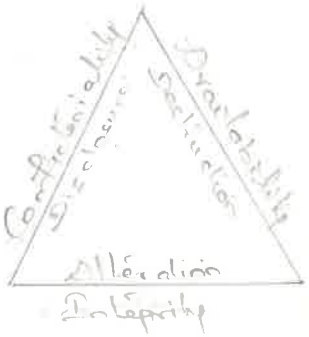
Meant By Decryption:?

Decryption is a process of converting encoding/encrypted data in a form that is readable/original and understood by a human or a Computer.

This method is performed by un-encrypting the text manually or by using keys used to encrypt the original data.

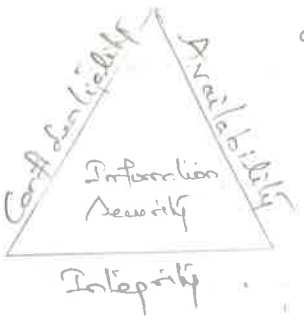
Security Goals:- UNIT-I

These three Concepts are termed as CIA triad and represent fundamental Security objectives for data and information services.



Security Goal:

Main goal of Security is to protect data or information which is being transmitted and achieve the Confidentiality, Integrity and availability of the data.



1. Confidentiality
2. Integrity
3. Availability

1. Confidentiality:-

✓ Principle of Security, which ensure that only the Sender & the receiver of a message come to know about the Content of message.

Ex:
- OTP for Banking transaction (Secure)
- Military application information from higher authority to another higher authority

✓ The attack threatening the Confidentiality is traffic analysis.

2. Integrity :

✓ Principle of security, which ensure that the content of message must not be altered/Modified during its transmission from sender to receiver.

✓ In this case change in the information need to is to be done by authorized person and through the authorized mechanisms only. ✓ Integrity gives assurance that the data received exactly as sent by an authorized sender.

✓ The attack threatening integrity is modification of message.

3. Availability:

✓ Principle of security, which ensure that a resource/ Computer system is available from authorized users only

✓ Information of bank account stored in the bank server.

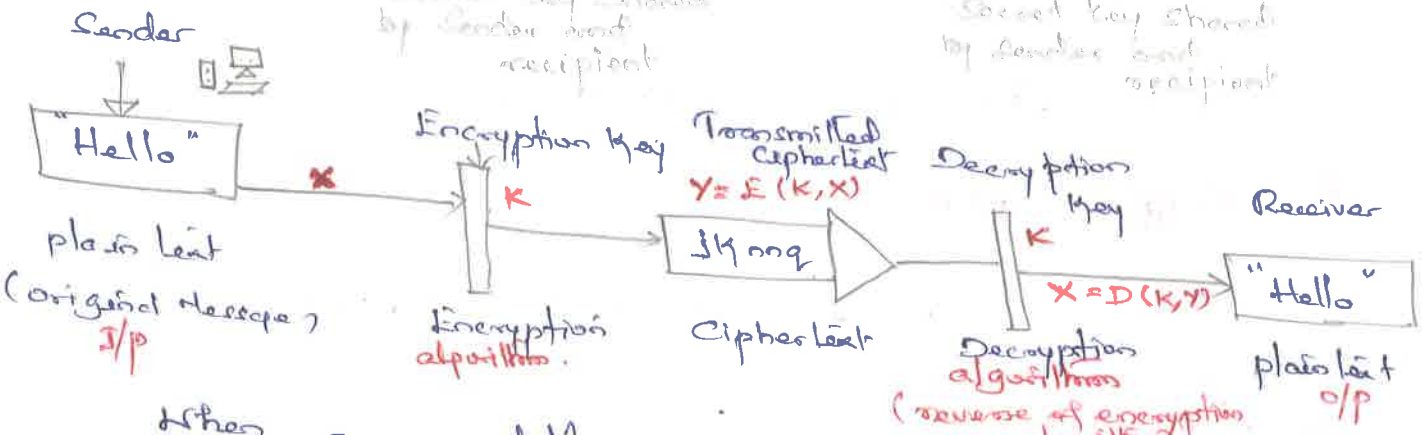
✓ Students information stored in University authorized server.

✓ All these information need to be available to all authorized users only.

✓ The above all information is not available to authorized user is one attack which threatening Principle of availability called denial of service.

Cryptography:

Cryptography is the art and science of achieving Security by encoding or encryption message to make them non-readable.



When a readable message is converted to a Unreadable message or outcome occured it is known as "Cipher text"

Basic terminology :-

1. **Plain text:** the original Message.

Plain text is nothing but known as the original message (the text that is not encrypted)

2. **Ciphertext:** the Coded message

The Coded message, the output of the encrypted process.

3. **Cipher:** the algorithm for transforming Plaintext to Ciphertext

The algorithm for transforming (ie; readable to Unreadable)

4. Key:

The information required to Convert the plain text and Cipher text

5. Crypt Analysis :- (or) Code breaking:

The method of ~~deciphering~~ (decryption) Ciphertext without knowing key.

Deciphering is nothing by decryption.

6. Cryptography :-

The art of designing Cipher. (Unknown format)

7. Cryptology :-

The both Combination of Cryptography and crypto analysis.

8. encipher :- (Encrypt)

To Converting plain text into the Cipher text.

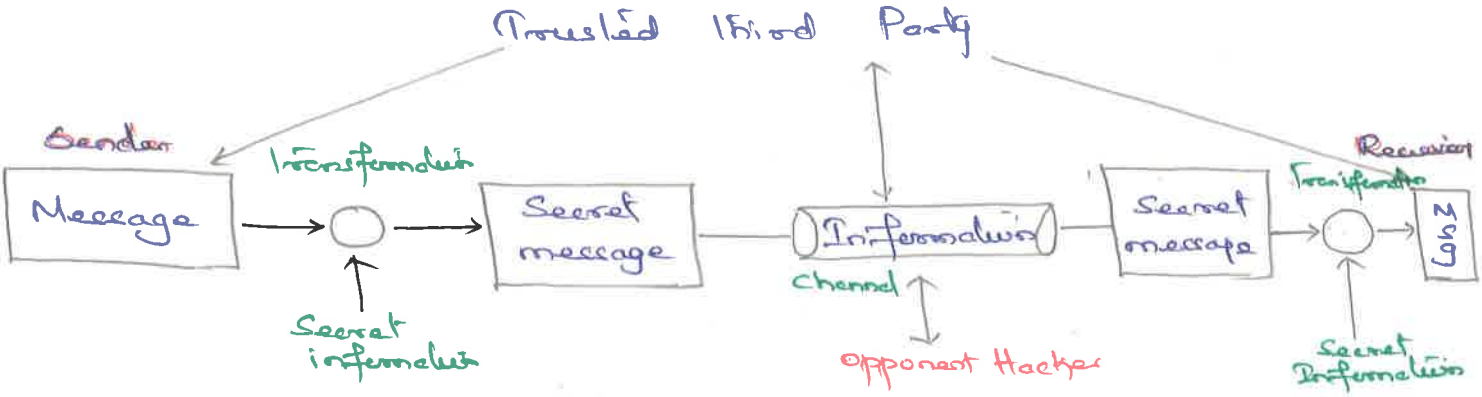
9. Decipher :- (Decrypt)

Reverse formation of Cipher text back into plain text.

These above nine of the Contents are the basic terminology Using in the network Security.

=.

Network Security :-



* The message is to be transfered from source to destination across some of internet that co-operate both the sides for exchanging data.
* A logical information channel is established by defining a root through the internet from source to destination
* All the techniques for providing security has two components:
  - Security related transformation on the information to be sent.
  - Some secret information shared by 2 principls. It is hidden, Unknown to opponent/ hacker.

Security Attacks :-

Defn:- A Cryptography attack is a method (or) technique used by hackers to target Cryptographic Solutions like
  - → Cipher text
  - → encryption keys

(Cryptographic attacks)

Security attacks.

Passive attacks

active attack.

Accessing of data by unauthorized entity is called as attacks.

Types of Security attacks:-

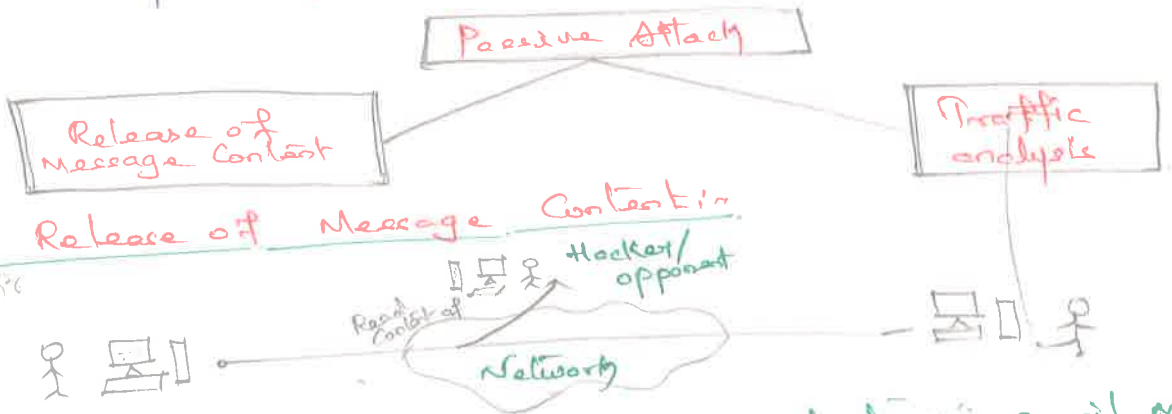
1. Passive attacks
2. active attacks

1. Passive attacks:

Def:- The attacker observes the Content of messages or Copys the Content of messages during the time of transmission over the network.

- The passive attack dangerous to Confidentiality
- Due to the passive attacks there is no harm to the system.
- The victim doesn't get informed about the attacks.
- It is difficult to detect.

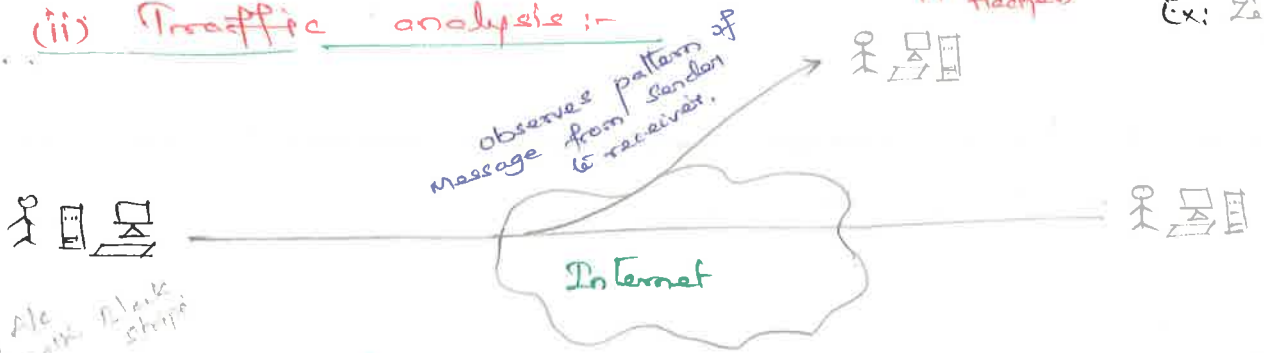
Two types of passive attacks.



(i) Release of Message Content:

- A telephone Conversation, an electronic email message and a transferred file may contain sensitive or Confidential information.
- we would like to prevent an opponent from learning the Content of these transmissions.

(iii) Traffic analysis :-



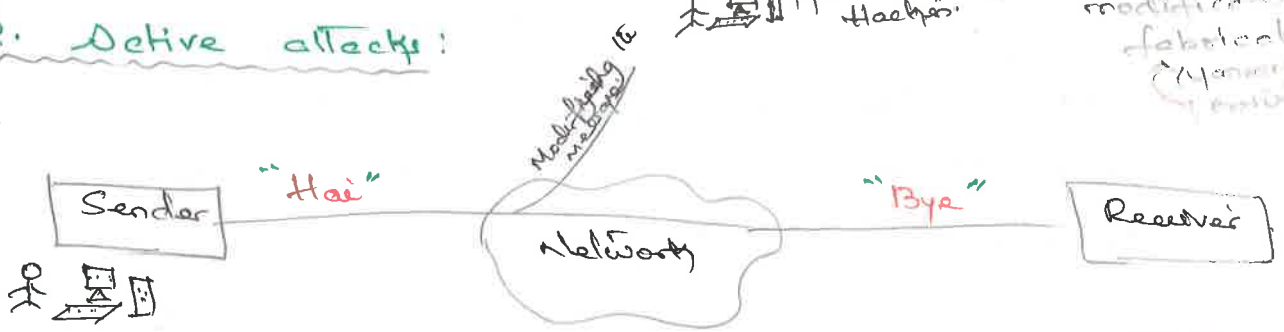
Ex: Zip file..

→ Mask - hide the Content of message, so that opponent Could not extract the information from the message.

→ The encryption is used for masking

→ The attacker observes the message but not open it and read it.

2. Active attacks :



(Interception/ modification/ fabrication)

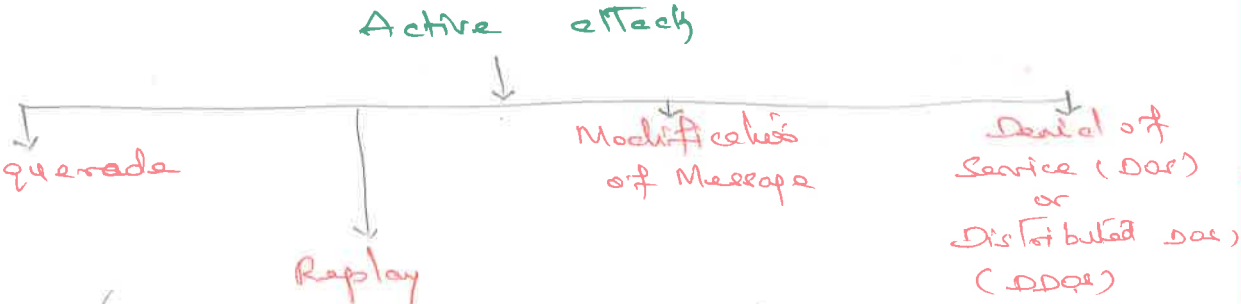
Defn: The attacker effort to change or modify the Content of the original message.

→ Due to active attack system is always damaged and the system resources can be changed

→ The active attack dangerous to data integrity as well as availability.

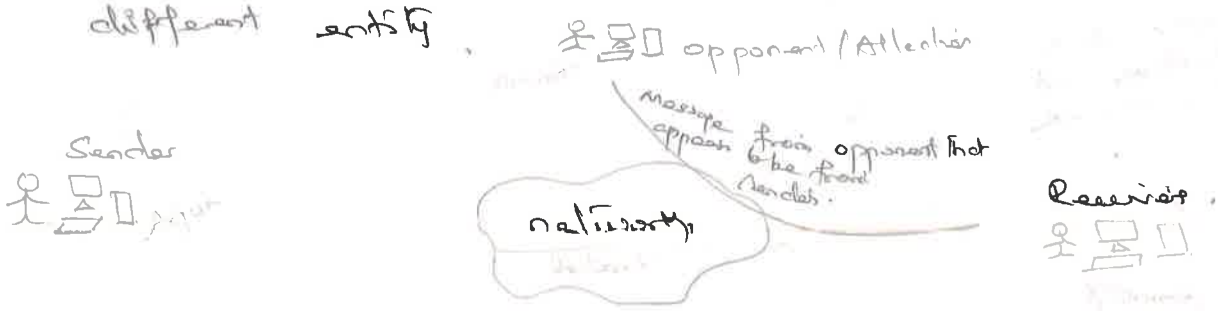
→ The victim gets informed about the attacks

There are categories into 4 parts:

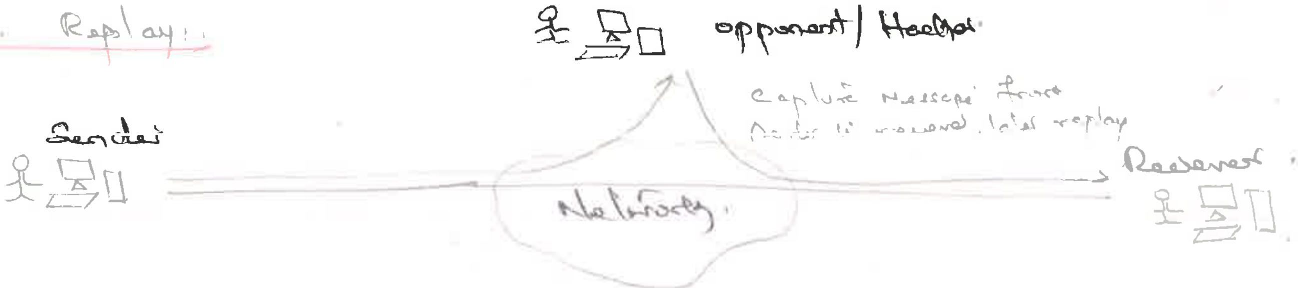


1. Masquerade :- Masquerade takes place when one entity pretends to be a different entity.

→ It takes place when one entity acts to be different entity.

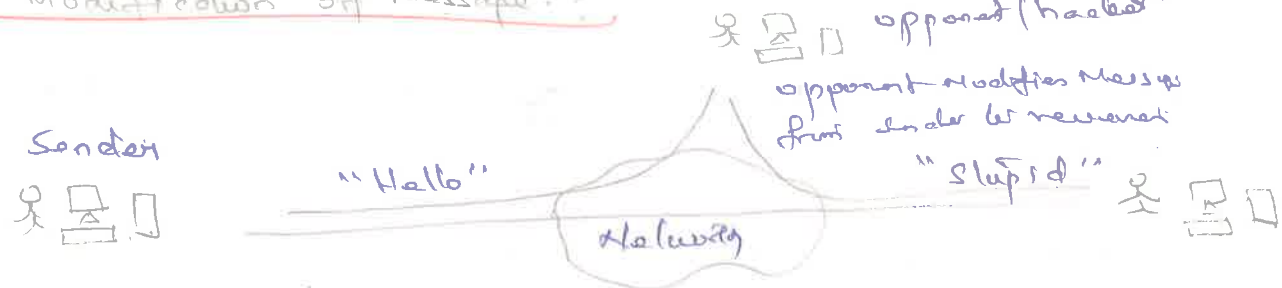


2. Replay :-



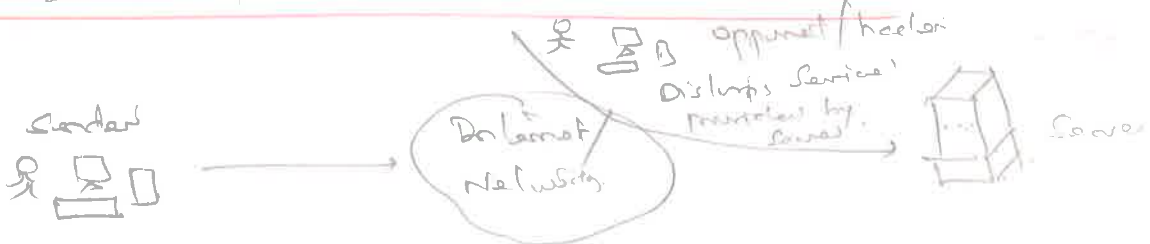
→ It involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.

3. Modification of Message :-



The content, It involves some changes to the original message it produces an unauthorized effect.

4. Denial of Service or (DoS attack)



→ The attackers directly attacking on the n/w and disturbs the n/w services between sender to receiver or receiver to sender.

→ The attack may have a specific target

Ex: URL (Uniform resource locator)

Types of DOS or DDOS Attacks :-

1. Penetration [injection or entering in the n/w]
2. Eaves dropping [attacker listens].
3. MITM [man - in - the - middle] attacks
4. Flooding [Attacker over flowing messages over the networks].

1. Penetration :

→ An attacker gets inside your Machine.
→ An attacker can take over the Machine and do whatever they need.
→ An attacker achieves only via Software flaws, stolen passwords.

2. Eaves dropping:

→ An attacker gains access of the same network
→ Listen through traffic going in and out of your Machine.

3. MITM Attacks: (man - in - the - middle)

→ An attacker listen to output and Control them.
→ Attacker will substitute message in both directions.

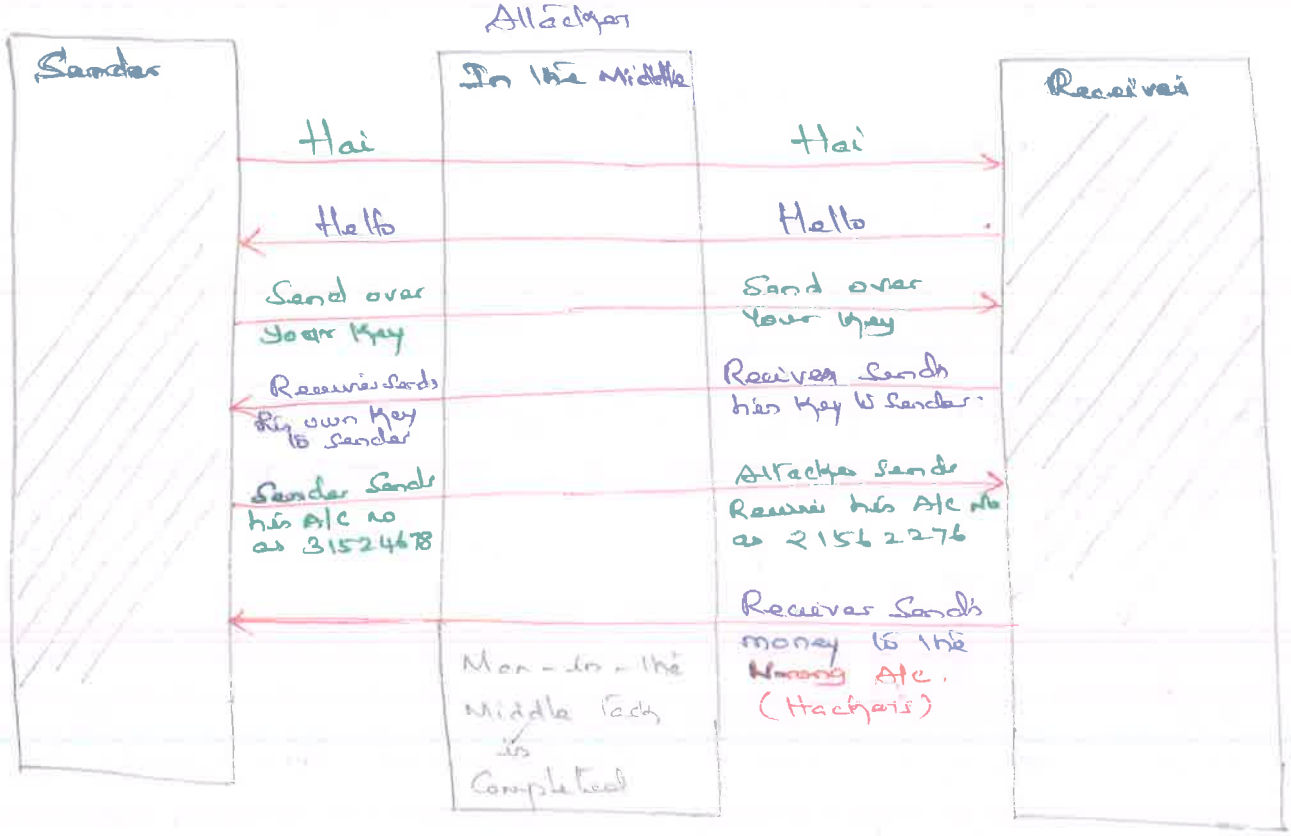
4. Flooding :-

→ An attacker sends a number of messages at your machine to form Congestion
→ Usually called as DOS - attack
→ Attacker Overflowing message over the network.

More about MITM :-

* A MITM is a form of Cyber attack
* An attacker involve between two parties and manipulates the message to achieve the target goal.

Diagram MITM :-

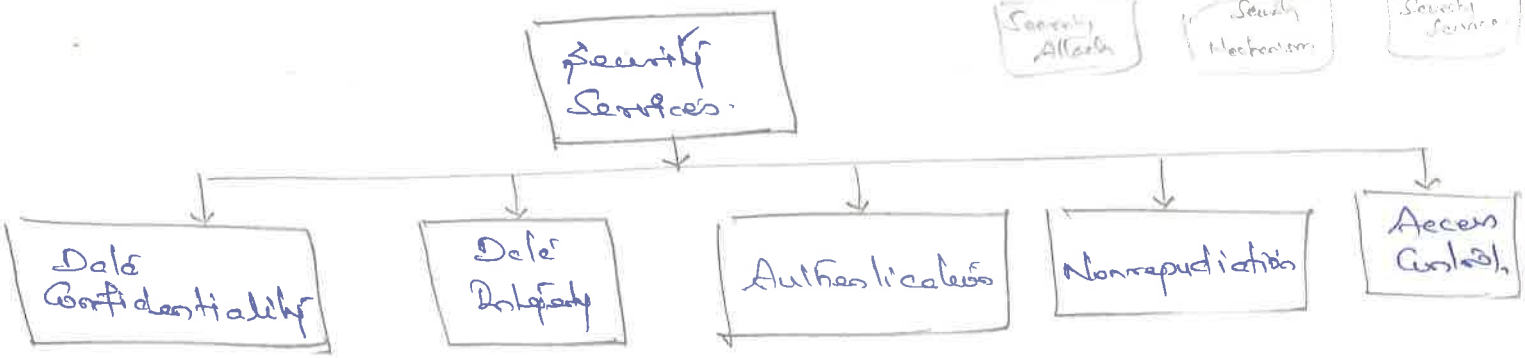


International Telecommunication Union

Services and Mechanism:

Security Services :-

ITU-T (X.800) is provided by protocol layer of transmission that defines Security Services ensures Security of the data transfer.



Data Confidentiality :- It is designed to protect data from disclosure attack, i.e. it is designed to Prevent Snooping and traffic analysis attack.

Data Integrity :- It is designed to protect data from modification, insertion, deletion and replaying by an adversary.

Authentication :- It provides the authentication of the party at the other end of the line.

Non-repudiation :- It protects against repudiation by either the sender or the receiver of the data.
i.e. Requires that neither the sender nor the receiver of a message be able to deny transmission

Access Control :- It provides protection against Unauthorized access to data.

Q1) [25, 150] ? GCD for this ?

	25	150
Divisors	1, 5, 25	1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150
Common Divisors	1, 5, 25	
GCD	25	

GCD (25, 150) = 25

1 | 25

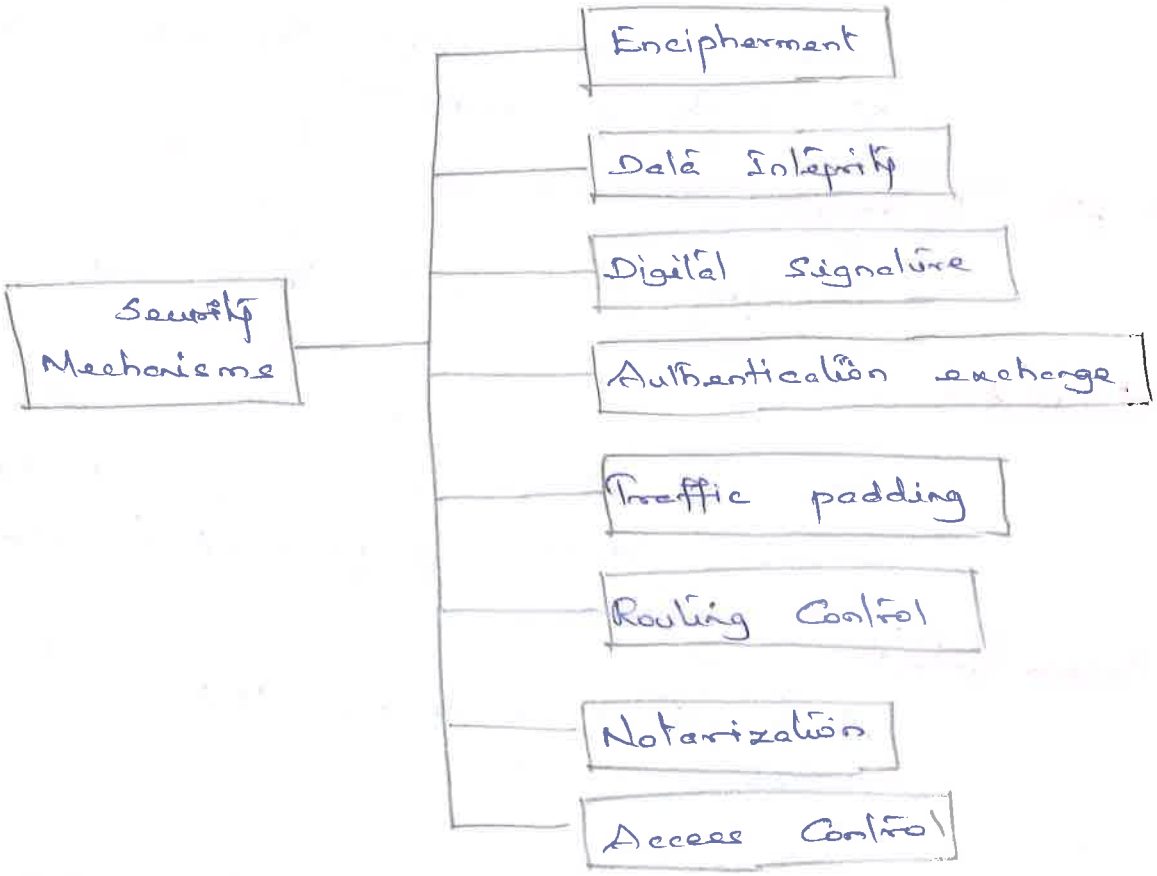
1 | 150

6 | 150

25

Security Mechanism:-

* Its a method or technique to prevent and detect the security attacks.
* ITU-T recommends Security mechanism to provide the Security Service.



Encipherment:

→ The use of mathematical algorithm to transform data that is not readily understandable.

Data Integrity:-

→ A variety of mechanisms used to assure the integrity of a data unit.

Digital Signature:-

→ The sender can electronically sign the data and the receiver can electronically verify the signature.

Authentication Exchange:-

→ A mechanism intended to ensure the identity of an entity by means of information exchange.

Routing Control :-

→ Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Traffic Padding :-

→ Inserting bogus data to prevent traffic analysis.

Notarization :-

→ The use of a trusted 3rd party to assure certain properties of a data exchange.

Access Control :-

→ A variety of mechanism that enforce access rights to resources

Services and Mechanisms:

X-800 defines a security service as a service, that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

RFC 4949

Provides: A processing or communication service that is provided by a system to give a specific kind of protection to system resources;

Security services implement security policies and are implemented by security mechanisms.

X.800 divides these services into the following categories:

1. Authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Non-repudiation
6. Availability Service

Authentication:

* Authentication service is concerned with assuring that a communication is authentic
* In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
* At the time of connection initiation, the service assures that authentic
* The service must assure that the connection is not interfered with that a third party for the purposes of unauthorized transmission.

Two specific authentication service in X.800.

1. Peer entity authentication.
2. Data origin authentication

1. peer Entity authentication:

Two entities are considered peers if they implement the same protocol in different systems.

Ex:- Two TCP modules in two communicating systems.

2. Data origin authentication.

Ensure the source of a data unit.

Mathematics of Cryptography:-

Algebric Structure:-

1. Groups
2. Rings
3. Fields

- Defn: A group G is a set of elements with a binary operation that satisfies four properties.

1. Groups:-

1) Closure property

$$c = a * b$$

$3 * 2 = 2 * 3$
$3 + 2 = 2 + 3$

2) Associative property

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

$(5 * 6) * 7 = 5 * (6 * 7)$
$(5 + 6) + 7 = 5 + (6 + 7)$

3) Identity

$$e * a = a * e = a$$

4) Inverse

$$a * a' = a' * a = e$$

Closure property:

If a and b are elements of G then $c = a * b$ is also an element of G. ie: $a, b \in G$

Associative Property:

If a, b & c are elements of G, then $(a * b) * c = a * (b * c)$ ie: $a, b, c \in G$

ie: $(3 * 2) * 4 = 3 * (2 * 4)$

Identity:- For all a in G there exist an element e called the identity element, $e * a = a * e = a$

ie: Ex: $1 * a = a * 1 = a$ $\quad e = 1$

Inverse:- For each a in G there exists inverse of a, an element a' called it as such that: $a * a' = a' * a = e$

II. Rings:

→ A ring denoted as $R = \langle \{\ldots\}, *, \square \rangle$ is an algebraic structure with two binary operations: '*', '□'

* The first operation '*' must satisfy all of the four properties

1) Closure property
2) associative property
3) Identity
4) Inverse

* The second operation '□' must for distributed for all a, b, c element of R.

5) Commutative property.

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

and

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

III. Field:-

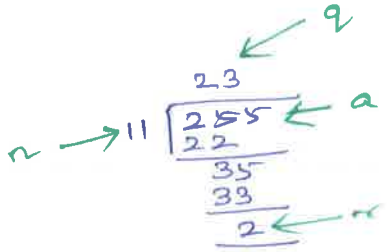
→ A field which is denoted by symbol 'F'

$F = \langle \{\ldots\}, *, \square \rangle$

→ Addition modular sets + Multiplication modular sets of two operations

e.g. F(7) or Z(7)

Modular Arithmetic:-



The division relationship

$$a = q \times n + r$$

Inputs: a and n

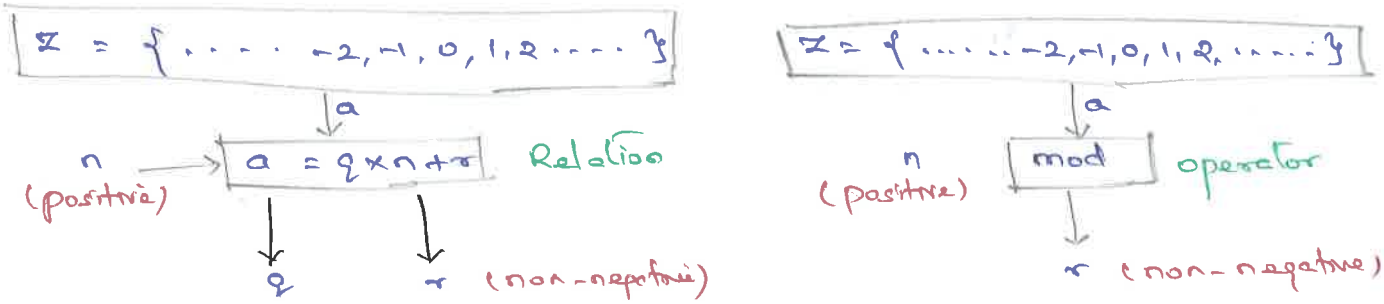
outputs: q and r.

In modular arithmetic we are focused in only one output

ie: Remainder r (output)

Modulo operator:

* mod can be used as modulo operator.
* Input n is modulus.
* output r is residue.



Division relation and modulo operator

* The modulo operator (mod) takes an integer (a) from the set Z and a positive modulus (n). The operator creates a non-negative residue (r).

$$a \bmod n = r$$

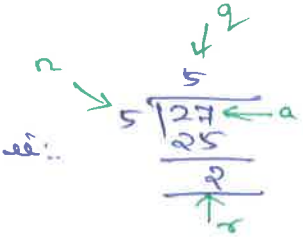
Examples:

(i) 27 mod 5 is ?

Qn: 36 mod 12 ?

Dividing 27 by 5 results in r = 2.

ie:



$$27 \bmod 5 = 2$$

(ii) −18 mod 14 is ?

Qn: −7 mod 10 ?

Dividing −18 by 14 results in r = −4. However, we need is add the modulus (14) to make it non-negative. we've r = −4 + 14 = 10, it gives $-18 \bmod 14 = 10$

Set of Residues : Z_n

* The modulo operation with modulus 'n' is always an integer between 0 and n-1.

* In other words a mod n is always a non-negative integer less than n.

* Modulus operation creates a set, that is called set of least residues modulo n or Z_n.

$$Z_n = \{0, 1, 2, 3, \ldots\ldots (n-1)\}$$

$Z_2 = \{0, 1\}$
$Z_3 = \{0, 1, 2\}$
$Z_4 = \{0, 1, 2, 3\}$

$Z_5 = \{0, 1, 2, 3, 4\}$
$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

The above are sets of Z_n.

Qn:1) Solve $10x \equiv 15 \pmod{15}$ Linear Congruence?

Qn:2) Solve $12x \equiv 16 \pmod{20}$ Linear Congruence? $x = 3 \bmod 5$

Obs:

$10x \equiv 15 \pmod{15}$

$2x \equiv 3 \pmod{3}$

$x = 0, 1, 2, 3 \ldots$

$2.0 \equiv 3 \pmod 3 = 0X$
$2.1 \equiv 3 \pmod 3 = 2X$
$2.2 \equiv 3 \pmod 3 = 1X$
$2.3 \equiv 3 \pmod 3 = 0X$
$2.4 \equiv 3 \pmod 3 = 2X.$
$2.5 \equiv 3 \pmod 3 = 1X.$
$2.6 \equiv 3 \pmod 3 = 0X.$
$2.7 \equiv 3 \pmod 3 = 2X.$
$2.8 \equiv 3 \pmod 3 = 1X$

$10x \equiv 15 \pmod{45}$

$2x \equiv 3 \pmod 9$

$2.0 \equiv 3 \pmod 9 = 0X$
$2.1 \equiv 3 \pmod 9 = 2X.$
$2.2 \equiv 3 \pmod 9 = 4X$
$2.3 \equiv 3 \pmod 9 = 6X.$
$2.4 \equiv 8 \pmod 9 = 8X$
$2.5 \equiv 3 \pmod 9 = 1X$
$2.6 \equiv 3 \pmod 9 = 3\checkmark$

$x = 6 \bmod 45$

$10x \equiv 15 \pmod{45}$ Solvable' gcd(10, 45) / 15
gcd (10, 45) / 5
ie 5/15

$2x \equiv 3 \pmod 9$

$x_0 = 6$

$x_0 = 6$; Sol: $10x \equiv 15 \pmod{45}$

$x' = x_0 + \frac{45}{5} \cdot t \quad ; \quad t : \{0, 1, \ldots 4\}$
$t : \{0, 1, \ldots n-1\}.$

$x' = 6 + \frac{45}{5}(0) = 6$
$x' = 6 + \frac{45}{5}(1) = 15$
$x' = 6 + 9(2) = 24$
$x' = 6 + 9(3) = 33$
$x' = 6 + 36 = 42$

$x' = 6, 15, 24, 33, 42 \pmod{45}$

Mathematics of Cryptography:

Integer Arithmetic:

We can use a set of a few operations.

The set of integers, denoted by $\mathbb{Z}$, contains all integer numbers (with no fraction) from $-\infty$ to $+\infty$.

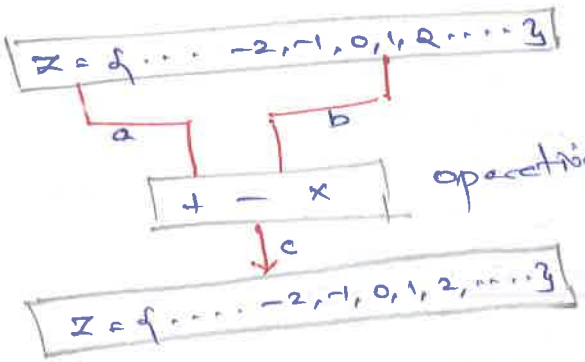
$$\mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2 \ldots \ldots \}$$

is known as the set of integers.

Binary Operations:

A binary operation takes two inputs and creates one output. Three common binary operations defined for integers are:

→ addition
→ subtraction
and
→ multiplication.



Ex: . Addition : $3+4 = 7$ $(-3)+4 = 1$ $+3+(-4) = -1$

Subtraction : $3-4 = -1$ $(-3)-4 = 7$ $+3-(-4) = 7$

Multiply : $3\times4 = 12$ $(-3)\times4 = -12$ $3\times(-4) = -12$

Integer Division:

If we divide a by n, we can get q and r.

This relation shows as:

$$a = q \times n + r$$

a is dividend.
n is divisor
q is quotient
r is remainder.

Assume a = 235, n = 11, we can find q = 23 and r = 2 using division algorithm

$$\begin{array}{r|l} & 21 \leftarrow q \\ \hline 11 & 349 \leftarrow a \\ & 33 \\ \hline & 19 \\ & 11 \\ \hline & 7 \leftarrow r \end{array}$$

n → 11

Congruence Modulo:

$52 \equiv 4 \pmod 8$

$a \equiv b \pmod n$

$52 - 4 = 48$ (Divisible by 8)

$a - b$ is divisible by n

52 ÷ 8 → 6, remainder 4

Linear Congruence:

$ax \equiv b \pmod m$

$12x \equiv 9 \pmod{21}$

$4 \times 3x \equiv 3 \times 3 \pmod{3 \times 7}$

$4x \equiv 3 \pmod 7$

$4 \cdot b \equiv 3 \pmod 7$

$x = 3 \bmod 7$

Qn: 1. Solve a linear Congruence ?

$12x \equiv 9 \pmod{21}$

$\Rightarrow 4x \equiv 3 \pmod 7$

$x = 0, 1, 2, 3, \ldots$

$4 \cdot 0 \equiv 3 \pmod 7 = 0$ ✗

$4 \cdot 1 \equiv 3 \pmod 7 = 4$ ✗

$4 \cdot 2 \equiv 3 \pmod 7 = 1$ ✗

$4 \cdot 3 \equiv 3 \pmod 7 = 5$ ✗

$4 \cdot 4 \equiv 3 \pmod 7 = 2$ ✗

$4 \cdot 5 \equiv 3 \pmod 7 = 6$ ✗

$4 \cdot 6 \equiv 3 \pmod 7 = 3$ ✓

$\therefore x = 6 \bmod 21$

$24 \equiv 3 \bmod 7$

Qn: 2: Solve a linear Congruence ? $9x \equiv 6 \pmod{15}$,

Soln. $9x \equiv 6 \pmod{15}$ is solvable as $\gcd(9, 15) \mid 6$

$ad \equiv bd \pmod n$

$a \equiv b \pmod n$.

$\gcd(d, n)$.

$3 \times 3x \equiv 2 \times 3 \pmod{5 \times 3}$

i.e. $3 \cdot 3x \equiv 2 \cdot 3 \pmod{5 \cdot 3}$

$3x \equiv 2 \pmod 5$

Let's take:

$3 \cdot 0 \equiv 2 \pmod 5 = 0$ ✗

$3 \cdot 1 \equiv 2 \pmod 5 = 3$ ✗

$3 \cdot 2 \equiv 2 \pmod 5 = 1$ ✗

$3 \cdot 3 \equiv 2 \pmod 5 = 4$ ✗

$3 \cdot 4 \equiv 2 \pmod 5 = 2$ ✓

$x = 0, 1, 2, \ldots$

$12 \equiv 2 \bmod 5$

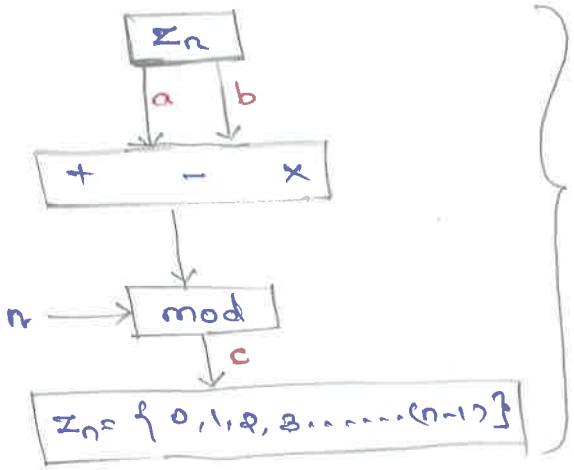
$\therefore x = 4 \bmod 15$

Note: $x = 4, 9, 14 \pmod{15}$

Operations in Z_n:

The Three Binary Operations
- addition
- Subtraction
- Multiplication

are defined for the set Z_n.



Binary operations in Z_n

operations:

$$(a+b) \bmod n = c$$
$$(a-b) \bmod n = c$$
$$(a \times b) \bmod n = c$$

Property: 1: $(a+b) \bmod n$

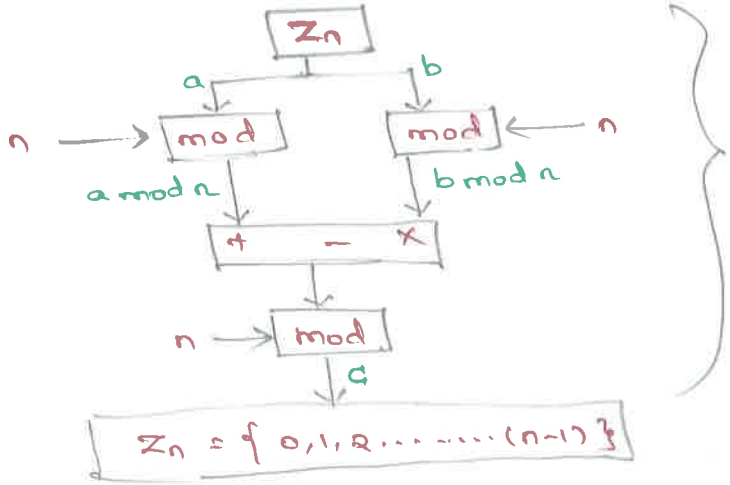
$= [a \bmod n + b \bmod n] \bmod n$

Property: 2: $(a-b) \bmod n$

$= [a \bmod n - b \bmod n] \bmod n$

Property: 3: $(a \times b) \bmod n$

$= [a \bmod n \times b \bmod n] \bmod n$



Apply the properties.

Qn: Perform the following operations from Z_n?

Ex: 1. add 7 to 14 in Z_{15}

Soln:

$(a+b) \bmod n = c$

$a = 14$

$b = 7$

$n = 15$

$= (14+7) \bmod 15$

$= 21 \bmod 15$

$= 6$ //

Qn: 2. add 15 to 24 in Z_{16}

$(a+b) \bmod n = c$

$a = 24$

$b = 15$

$n = 16$

$= (24+15) \bmod 16$

$= 39 \bmod 16$

$= 7$ //

16 | 39 (2, 32, 7)

Ex: add 17 to 27 in Z_{14}.

add 8 & 12 in Z_9

$= (10+8) \bmod 9$

$= 18 \bmod 9$

$= 0$ //

9 | 18 (2, 18, 0)

Ex: 1. Subtract 11 from 17 in Z_{13}

$(a-b) \bmod n = c$

$= (17-11) \bmod 13$

$= 6 \bmod 13$

$= 6$ //

Qn: Subtract 5 from 12 in Z_9

Subtract 12 from 20 in Z_{14}

2. Subtract 34 from 12 in Z_{13}

$(a-b) \bmod n$.

$= (12-34) \bmod 13$

$= (-22) \bmod 13$

$= -9$

$= -9+13$

$= 4$

13 | -22 (-1, 13, -9)

$a = qxn+r$

$a = 1 \times 13 + 4$

$a = 13+4$

$a = 17$

13 | 17 (1, 13, 4)

Ex: 1. Multiply 11 by 7 in Z_{20}

$(a \times b) \bmod n = c$

$a = 7$

$b = 11$

$n = 20$

$= (7 \times 11) \bmod 20$

$= 77 \bmod 20$

$= 17$

20 | -1230 (-61, 120, -30, 20, -10)

2. multiply 123 by -10 in Z_{20}

$a = -10$

$b = 123$

$n = 20$

$\Rightarrow (-10 \times 123) \bmod 20$

$= -1230 \bmod 20$

$= -10 + 20 = 10$ //

Ex: perform the following operation

1. add 17 to 27 in Z_{14}
2. Subtract 34 from 12 in Z_{13}
3. Multiply 123 by -10 in Z_{20}

Soln

$= 123 (-10) \bmod 20$

$= -1230 \bmod 20$

$= -10 + 20$

$= 10$

20 | -1230 (-61, 120, -30, 20, -10)

Property 1:

$$(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$

Qn: Add 7 to 12 in Z_{13}

$a = 12 \quad b = 7 \quad n = 13$

$(12+7) \bmod 13 = [(12 \bmod 13) + (7 \bmod 13)] \bmod 13$

$19 \bmod 13 = (12+7) \bmod 13$

$6 = 19 \bmod 13$

$6 = 6$

Property 2:

$$(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$

Qn: Subtract 5 from 4 in mod 2 or Z_2

$a = 4 \quad b = 5 \quad n = 2$

$(4-5) \bmod 2 = [(4 \bmod 2) - (5 \bmod 2)] \bmod 2$

$2 \overline{)-1}$ = NOT

$-1 \bmod 2 = (0-1) \bmod 2$

$-1 \bmod 2 = -1 \bmod 2$

$-1 = -1$

Property 3:

$$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

Qn: Multiply 6 by 9 in Z_{18}

$a = 9 \quad b = 6 \quad n = 18$

$(9 \times 6) \bmod 18 = [(9 \bmod 18) \times (6 \bmod 18)] \bmod 18$

$54 \bmod 18 = [(9 \times 6) \bmod 18]$

$54 \bmod 18 = 54 \bmod 18$

$0 = 0$

$18 \overline{)54}$ (3), 54, 0

* gcd (24, 30, 36) = 6
* gcd (20, 15, 10) = 5
* gcd (45, 210) = 15
* gcd (36, 60) = 12

Common division:

$2 \overline{)36, 60}$
$2 \overline{)18, 30}$
$3 \overline{)9, 15}$
$3, 5$

$2 \times 2 \times 3 = 12$

Modulo operation:

1. $17 \bmod 2 = ?$
2. $15 \bmod 4 = ?$
3. $-11 \bmod 7 = ?$
4. $-15 \bmod 2 = ?$
5. $-27 \bmod 10 = ?$
6. $-56 \bmod 5 = ?$

Additive Inverse:-

—— do ——.

Given Qn: find MI of 11 in Z_{26}?

$t_1 = 1 \quad t_2 = 0$

$t = t_1 - t_2 \times q.$

$= 1 - 0 \times 0$

$= 1$

q	r_1	r_2	t_1	t_1	t_2	t
0	11	26	~~11~~	1	0	1
	26	11		0	1	

gcd = 1

$-7 \bmod 26$

$= 19$

In Cryptography:- Z_p and Z_p^*

Z_p :- The modulus is:- n is prime number,

So the table Z_p, It has additive inverse.

p Contains all integers from 0 to p-1

Z_p^* :- Z_p^* is inverses as Z_n^*, But n is prime,

The set Contains multiplicative inverse.

it: all integers from 1 to p-1 //.

it:- We need to use Z_n set when additive inverses are needed

Ex:- Set Z_6 is 0 to p-1

$Z_6 = \{0, 1, 2, 3, 4, 5\}$.

We need to use Z_n^* set when Multiplicative inverses are needed.

Ex:- Set Z_6^*

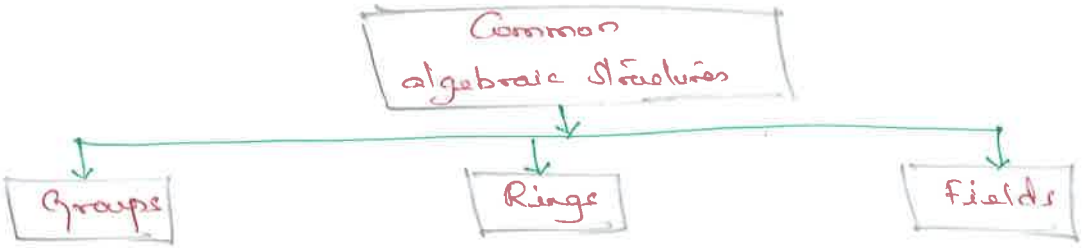
$Z_6^* = \{1, 5\}$

Algebraic structures:

Cryptography requires sets of integers and specific operations that are defined for these sets. The combination of the set & the operations that are applied to the elements of the set is called an algebraic structure.

Three common algebraic structures:

- → Groups
- → rings &
- → fields



Modular Arithmetic:

$a \% n$

$n \mid a$

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus.

Properties of modulo operator:

Congruences have the following:

1. $a \equiv b \pmod n$ if $n/(a-b)$
2. $a \equiv b \pmod n$ implies $b \equiv a \pmod n$
3. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$

Groups, Rings and Fields:

Groups, rings and fields are the fundamental elements of a branch of mathematics known as abstract algebra or Modern algebra.

Groups:

A group G, denoted by $\{G, \cdot\}$ 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 obeyed.

(i) closure: if a and b belongs in G.

then

$a \cdot b$ is also in G.

(ii) Associative:

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

(iii) Identity element:

There is an element e in G s.t

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

(iv) Inverse element.

For each a in G, there is an element a^{-1} in G.

such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

(v) Commutative: $a \cdot b = b \cdot a$ $\forall$ a, b in G.

Mathematics of Cryptography:

① Find inverse matrix A ?

$$A = \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix}_{2\times 2 \text{ matrix}}$$

Step 1: Find the determinant of matrix A.

$$\det A = \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix}$$

$$= 28 - 30$$

$$= -2$$

Formula:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

The determinant of $A = ad - cb$

Step 2: Find the adjoint of Matrix A.

$$A = \begin{bmatrix} 4 & 5 \\ 6 & 7 \end{bmatrix}$$

$$\text{adj } A = \begin{bmatrix} 7 & -5 \\ -6 & 4 \end{bmatrix}$$

Formula

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\text{adj } A = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Step 3: Using the following formula to find A^{-1} is.

$$A^{-1} = \frac{1}{|A|} \text{adj } A \quad (\text{or}) \quad \frac{1}{\det A} \text{adj } A$$

w.k.t det A and adj A.

Now we can apply it.

$$A^{-1} = \frac{1}{-2} \begin{bmatrix} 7 & -5 \\ -6 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} -7/2 & 5/2 \\ 6/2 & -4/2 \end{bmatrix}$$

$$= \begin{bmatrix} -7/2 & 5/2 \\ 3 & -2 \end{bmatrix}$$

(or)

$$= \begin{bmatrix} -3.5 & 2.5 \\ 3 & -2 \end{bmatrix} //.$$

(2) Matrix Multiplication :-

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \qquad B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$$

$$A \times B = \begin{bmatrix} 1\times5+2\times7 & 1\times6+2\times8 \\ 3\times5+4\times7 & 3\times6+4\times8 \end{bmatrix}$$

$$= \begin{bmatrix} 5+14 & 6+16 \\ 15+28 & 18+32 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix} //$$

(3) Matrix addition :-

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \qquad B = \begin{bmatrix} 3 & 4 \\ 5 & 6 \end{bmatrix}$$

$$A+B = \begin{bmatrix} 2+3 & 1+4 \\ 3+5 & 2+6 \end{bmatrix} = \begin{bmatrix} 5 & 5 \\ 8 & 8 \end{bmatrix} //$$

(4) Matrix Subtraction :-

$$A = \begin{bmatrix} 4 & 3 \\ 2 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 3 & 0 \\ 1 & -2 \end{bmatrix}$$

$$A-B = \begin{bmatrix} 4-3 & 3-0 \\ 2-1 & 1+2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix} //$$

(5) Euclidean Algorithm :- (GCD) or (HCF)

Greatest Common Divisor
Highest Common (or) Common Factor

Ex:- [12, 33] ? GCD for Composite numbers ?

	12	33
Divisors	1, 2, 3, 4, 6, 12	1, 3, 11, 33
Common Divisors	1, 3	
Greatest Common Divisor	3	

$\therefore$ GCD (12, 33) = 3 //

12 | 12 / 1 | 1 | 12 / 12
2 | 12 / 2 | 6 / 3 | 2 | 12 / 2 | 4 / 2 | 4 | 12 / 3
6 | 12 / 2
1 | 33 / 33 | 2 | 33
3 | 33 / 11 | 4 | 33 | 5 | 33
6 | 33 . . 33 | 33 / 1

Matrices:

A matrix is a (1xj) elements can be arranged in row and column in a rectangular array.

n is number of rows and m is number of column.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{32} \end{bmatrix}_{3\times3}$$

Ex: $\begin{bmatrix} 1 & 5 & 6 \end{bmatrix}_{1\times3}$ - Row matrix.

$\begin{bmatrix} 2 \\ 9 \\ 11 \end{bmatrix}_{3\times1}$ - Column matrix.

$\begin{bmatrix} 32 & 1 & 15 \\ 4 & 0 & 3 \\ 8 & 10 & 13 \end{bmatrix}_{3\times3}$ - Square matrix. (Equal no: of rows & column.)

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}_{3\times2}$ - Zero matrix. (All the elements are zero).

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2\times2}$ - Identity Matrix. [Except diagonal element all other are zero].

Some of the operations:

1. Matrix addition
2. Matrix Multiplication
3. Matrix Subtraction
4. Scalar multiplication

Addition: Addition of two Matrix $C = A + B$

Multiplication: Multiplication of two Matrix. $C = A \times B$

Subtraction: Subtraction of two Matrix. $C = A - B$

Scalar: Multiple any element with matrix $C = xA$ or $C = xB$

Determinant of Matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$= a_{11} \times a_{22} - a_{12} \times a_{21}$$

Additive Inverse:

Number + Additive inverse = 0

Ex: $5 + (-5) = 0$

$-\frac{5}{9} = \frac{5}{9}$

ex: $-\frac{5}{9} + \frac{5}{9} = 0$ //

Multiplicative Inverse:

Ex: $3 \rightarrow \frac{1}{3}$

$\frac{2}{3} \rightarrow \frac{3}{2}$

$-1/5 \rightarrow -5$

Inverse Matrix:-

1. Additive Inverse
2. Multiplicative Inverse

Qn: Find MI of 11 in Z_{26} ?

11, 26

Greatest is r1

Smallest is r2

Initially

$t_1 = 0$

$t_2 = 1$

$t = t_1 - t_2 \times q$

q	r_1	r_2	r (remainder)	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
x	1	0	x	-7	26	x

gcd(1)

MI = -7

$\frac{1}{0} = \infty$

$-7 + 26 = 19$

Positive point = 19

negative point = -7

Multiplicative Inverse is 19 or -7 //

Qn: Find MI of 2 in Z_7 is = 4

Qn: Find MI of 4 in Z_{11} is = 3

(a)

q	r_1	r_2	r	t_1	t_2	t
3	7	2	1	0	1	-3
2	2	1	0	1	-3	7
x	1	0	x	-3	7	x

-3+7=4

MI is 4

(b)

q	r_1	r_2	r	t_1	t_2	t
2	11	4	3	0	1	-2
1	4	3	1	1	-2	3
3	3	1	0	-2	3	-11
x	1	0	x	3	-11	x

MI is 3

Abroad

Additive Inverse in Cryptography:-

Additive Inverse of $\frac{1}{3} = -\frac{1}{3}$

" $-\frac{1}{3} = \frac{1}{3}$

" $5 = -5$

" $-5 = 5$

" $-\frac{13}{8} = \frac{13}{8}$

" $\frac{13}{8} = -\frac{13}{8}$

Abroad

Multiplicative Inverse of $3 \rightarrow \frac{1}{3}$

" $\frac{2}{3} \rightarrow \frac{3}{2}$

" $-\frac{1}{5} \rightarrow -5$

" $\frac{4}{7} \rightarrow \frac{7}{4}$