

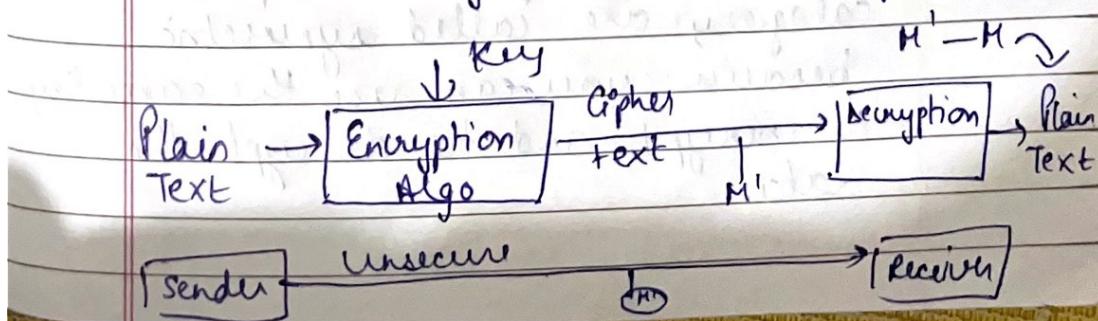
Cryptography

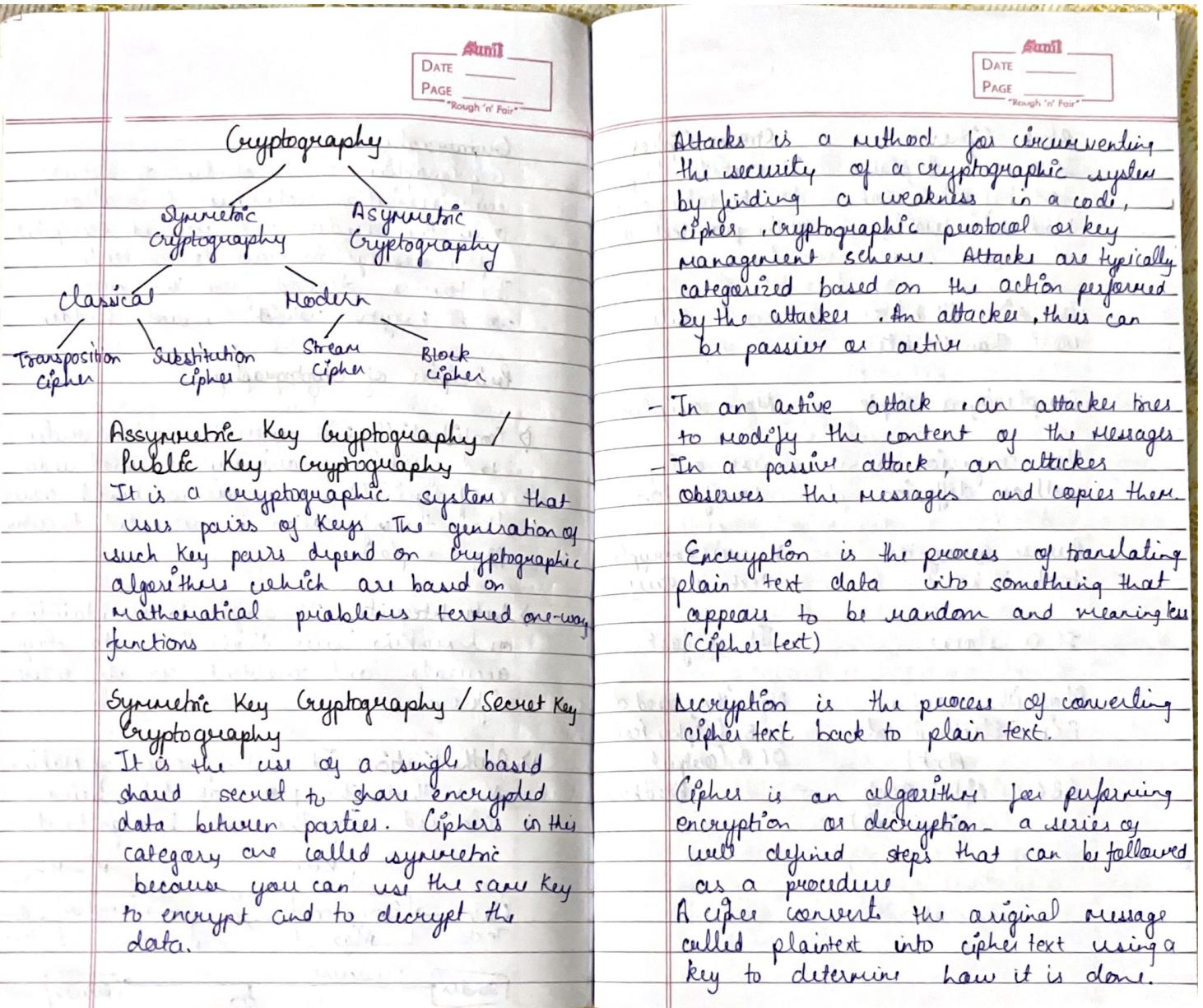
Cryptography is the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents.

The term is derived from the greek word Kryptos which means hidden

Principles of Cryptography

- 1) Confidentiality: It refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places
- 2) Data Integrity: It refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
- 3) Authentication: It is the process of making sure that the piece of data being claimed by the user belongs to it.





Block Cipher

It converts the plain text by taking each block individually.

Uses either 64 bits or more than 64 bits

Complexity is simple

Uses confusion as well as diffusion

Reverse encrypted text is hard

It is slow

Algorithms used are ECB (Electronic Code Block)

CBC (Cipher Block Chaining)

Stream Cipher

It converts the plain text by taking one byte of the plaintext at a time.

uses 8 bits

More complex

uses only confusion

Reverse encrypted text is easy

It is fast

Algorithms used are CFB (Cipher Feedback)

OFB (Output Feedback)

Bit

Smallest unit of computer information. It's essentially a single binary data point, either yes or no on or off, up or down.

Byte

Unit of memory that usually contains 8 bit. This is because historically, 8 bits are needed to encode a single character of text.

Cryptography is the science of writing in secret code so that no other person except the intent recipient could read.

Crypto means hidden secret and graphic means to write or study

Cryptography is the practice and study of technique for secure communication in the presence of third party.

More generally it is about constructing and analysing protocols that overcome the influence of attacker or outside people and which are related to various aspect in information security such as data confidentiality, data integrity, authentication.

Sumit
DATE _____
PAGE _____
"Rough 'n' Fair"

Applications of Cryptography
It includes ATM cards, computers, passwords, etc.

It is the science of using mathematics to encrypt or decrypt the data. It enables you to store sensitive info or transmit it across insecure channel (networks).

Types of Cryptography

1) **Symmetric Key Cryptography (Same Key)**
Private / Secret Key Cryptography

Key methods - DES, 3DES, AES

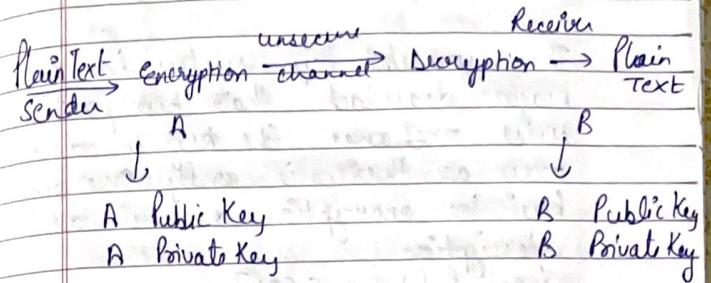
Plaintext
sender → Encryption ^{unsecure} channel → Decryption ^{Receiver} → Plain text
(we use various algorithms)

$$C [K1[M]] \xrightarrow{\text{cipher text}} M = [K1[C]]$$

C = Cipher Text
K1 = Key
M = Message (Plain Text)

public key is broadcast at any point of time

2) Asymmetric Key Cryptography (Public Key Cryptography)



Cases

- 1) $A = E [A \text{ Public Key } [M]] \text{ send to } B$ X
- 2) $A = E [B \text{ Private Key } [M]] \text{ send to } B$
- 3) $A = E [A \text{ Private Key } [M]] \text{ send to } B$ X

→ confidentiality not achieved

- 4) $A = E [B \text{ Public Key } [M]] \text{ send to } B$

Always use receiver public key to encrypt the message.

Symmetric Key Cryptography
Also known as private key / secret key cryptography

In symmetric key cryptography a single key is used for both encryption & decryption

AES (Advanced Encryption System) uses widely used symmetric key cryptography (AES, 2AES, 3AES)

The symmetric key system has one major drawback that two parties must exchange the key in a secure way as there is only one single key for encryption as well as decryption

$$i.e. P = [K(x, E(P))]$$

where K - Key for both (encryption & decryption)

P = Plain Text

D = Decryption

E(P) = Encryption for Plain Text

Stenography

The action or process of writing in shorthand and transcribing the shorthand on a typewriter

Advantages of Symmetric

- It is faster
- encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted

Since there is no key transmitted with

the data, the chances of data being decrypted are null.

- A symmetric uses password authentication to prove the receiver's identity.
- A system only which possesses the secret key can decrypt a message.

Disadvantages of Symmetric

- Have a problem of Key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

- cannot provide digital signatures that cannot be repudiated.

Advantages of Asymmetric

- In this, there is no need for exchanging keys, thus eliminating the key distribution problem
- Increased security: the private key do

not ever need to be transmitted or revealed to anyone

- can provide digital signatures that can be repudiated.

Disadvantages of Asymmetric
for encrypting this method is slow
there are popular secured-key encryption methods which are significantly faster than any currently available public-key encryption method.

Security Services

Confidentiality

Integrity

Authentication \rightarrow (password)

Non-repudiation \rightarrow (proof of access)

Access control

Asymmetric Key Cryptography
Also known as public key or conventional cryptography

In this two keys are used for encryption and decryption

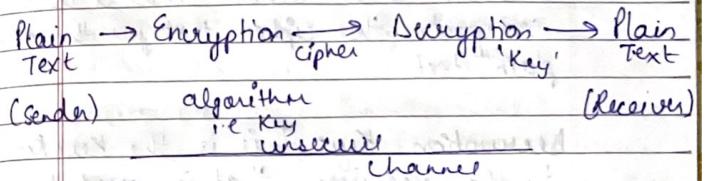
$$P = D(K_d, E(K_e, P))$$

Cryptosystem

A system which converts plain text to cipher text by the application of encryption or decryption algorithms

The key generation for encryption & decryption algorithm is also a part of a cryptosystem

A cryptosystem is an implementation of cryptographic techniques



Plain Text : This is the data that needs to be protected

Encryption Algorithm : This is the mathematical algorithm that takes plain text as the input and return cipher text.

It also produce the unique encryption key for the text.

Cipher Text : This is the encrypted or

unreadable form of the plain text

Decryption Algorithm: This is the mathematical algorithm that takes cipher text as the input and decodes it into plain text or original text.

It also uses the unique decryption key for the text.

Encryption Key: This is the value known to the sender that is used to compute the cipher text for the given plain text.

Decryption Key: This is the key known to the receiver that is used to decode the given cipher text to plain text.

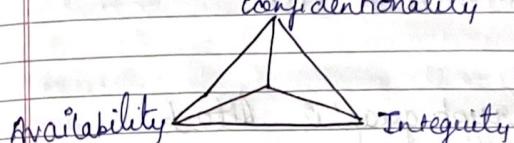
Challenges of Symmetric Key Cryptography

1) **Key Establishment:** Before any communication both the sender and the receiver needs to agree on a secret symmetric key.

2) **Trust Issue:** Since the sender and

- the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver trust each other.

Security Goals - CIA Triad in Cryptography
confidentiality, availability, integrity



- Confidentiality (privacy): It is the most common aspect of information security. It allows authorized users to access sensitive and protected data. The data sent over the network should not be accessed by unauthorized users.
- Availability: Attackers will try to capture the data so to avoid this various encryption techniques are used to save our data so that even if attackers gain access to the data they will not be able to decrypt it.
- Integrity: means that changes need to be done

Integrity

means that changes need to be done

Information is useless if we cannot access it
what would happen if we cannot access my
bank account for transaction?

DATE _____
PAGE _____
"Rough 'n' Fair"

by the authorized entity and
through authorized mechanisms.
and nobody else should modify
our data.

Availability

Data must be available to the
authorized user.

Cryptographic Attack

Cryptanalytic Attack

eg (Bruteforce attack)
tools → Hydra, crack

Hacking small passwords

(Dictionary attack)

Hacking long length
passwords

Non-Cryptanalytic Attack

eg (Security attack)

L security attack

L security mechanism

L security services

II applied on CIA

✓ ↘ ↙

passive active

Attacks

Attack is any attempt to explore,
alter, destroy, steal or gain information
through unauthorized access

Bruteforce attack

It uses trial and errors to guess
logging information, encryption keys,
or find a hidden web page
eg - crack, hydra, rainbow crack etc

Security Dictionary attack

It is a password-guessing technique
by trying many common words and
their simple variations. Attackers use
extensive lists of the most commonly
used passwords, popular pet names,
literally just words from a
dictionary

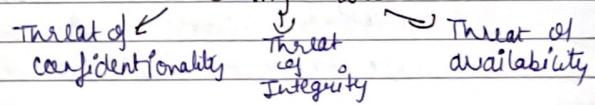
Security Attack. (for standard)

OSI security model focus on three
basic aspect of network security.

- security attack
- security mechanisms
- security services

Three goals of security (CIA) can be
threatened by security attacks.

Security Attack



Threat of Confidentiality

- Snooping
- Traffic analysis

Snooping: It is unauthorized access to data or information.

Traffic analysis: we encrypt the information, so that the attacker even if captured the message, could not extract any information from the message.

- eg → net flow analyser
- Microsoft message analyser

Threat to Integrity

- Modification
- Masquerading attack
- Replay attack
- Repudiation

Modification

After accessing the information the attacker alter the message or that message could be delayed or deleted done by unauthorized user.

Masquerading attack (Spoofing)

It happens when the attacker impersonates somebody else i.e. one entity pretend to be a different entity.

eg → a user try to contact a bank but another site pretend that it is the bank and obtained info.

Replay attack (playback attack)

The attacker obtained a copy of a message send by a user and later try to replay or resend or delay it.

eg → text dependent speaker verification.

Repudiation

It can be done by the sender or receiver. The sender of the message might later deny that he has sent the message, the receiver might later deny that he has received the message.

Threat of Availability

Denial of service (DoS)

An attempt to make a server or

Machines or network resources unavailable to its intent user.

Security Attack

- Passive
- Active

Passive Attack

It attempt to learn or make use of the information from the system but does not affect the system resources i.e. the attacker will only see the data, he will not modify it.

To prevent, we can prevent it using encryption techniques

Types of Passive attacks

- 1) Release of Message content

Eg- Brute-force attack

The attacker will easily be able to understand the data or information

- 2) Traffic Analysis

If we have encryption protection and attacker might still be able to see the pattern of these messages

The attacker could determine the location and identify of communication host and could absorb the frequency and length of the message being exchanged

Active Attack

Active attack - it attempt to alter the system resource and information. It involve some modification of data stream or creation of false statement.

Caesar cipher Encryption

$$EM(n) = (n + k) \text{ Mod } M$$

value of Key
particular letter.

Modulus
Max limit of set

Zayn will sing a song
Key = 7

$$G h f u c p t z p y n h z V y n \\ = (25+7) \text{ Mod } 26 \quad (2)$$

$$= 32 \text{ Mod } 26$$

$$= 6 \quad (g)$$

$$D = (0+7) \text{ Mod } 26 \quad (a) \\ = 7 \quad (d) \quad (h)$$

$$3) E = (24+7) \text{ Mod } 26 \quad (y) \\ = 5 \quad (f)$$

Amrit
DATE _____
PAGE _____
"Rough 'n' Fair"

$$\begin{aligned}
 4) &= (19+7) \bmod 26 \quad (n) \\
 &= 26 \quad (y) \\
 \\
 5) &= (22+7) \bmod 26 \quad (w) \\
 &= 3 \quad (d) \\
 \\
 6) &= (8+7) \bmod 26 \quad (i) \\
 &= 15 \quad (p) \\
 \\
 7) &= (11+7) \bmod 26 \quad (e) \\
 &= 18 \quad (s) \\
 \\
 8) &= (14+7) \bmod 26 \quad (s) \\
 &= 21 \quad (z) \\
 \\
 9) &= (6+7) \bmod 26 \quad (g) \\
 &= 13 \quad (n) \\
 \\
 10) &= (14+7) \bmod 26 \quad (o) \\
 &= 21 \quad (v)
 \end{aligned}$$

Caesar cipher Decryption
 $D_M(v) = (v-k) \bmod M$

We shall overcome
px lathee hoxkvhfx

Amrit
DATE _____
PAGE _____
"Rough 'n' Fair"

$$\begin{aligned}
 1) W &= (22-7) \bmod 26 \\
 &= 15 \bmod 26 \\
 &= 41 \bmod 26 \\
 &= 15 \quad (p) \\
 \\
 2) R &= (11-7) \bmod 26 \\
 &= 4 \bmod 26 \\
 &= 30 \bmod 26 \\
 &= 4 \quad (e) \\
 \\
 3) E &= (4-7) \bmod 26 \\
 &= -3 \bmod 26 \\
 &= 23 \bmod 26 \\
 &= 49 \bmod 26 \\
 &= 23 \quad (x) \\
 \\
 4) S &= (18-7) \bmod 26 \\
 &= 11 \bmod 26 \\
 &= 37 \bmod 26 \\
 &= 11 \quad (l) \\
 \\
 5) H &= (7-7) \bmod 26 \\
 &= 0 \bmod 26 \\
 &= 26 \bmod 26 \\
 &= 0 \quad (a) \\
 \\
 6) A &= (0-7) \bmod 26 \\
 &= -7 \bmod 26 \\
 &= 19 \bmod 26 \\
 &= 35 \bmod 26 \\
 &= 19 \quad (t)
 \end{aligned}$$

#unit
DATE _____
PAGE _____
"Rough 'n' Fair"

7) $o = (14-7) \bmod 26$
 $7 \bmod 26$
 $33 \bmod 26$
 $7 \quad (h)$

8) $v = (21-7) \bmod 26$
 $14 \bmod 26$
 $40 \bmod 26$
 $14 \quad (o)$

9) $u = (17-7) \bmod 26$
 $10 \bmod 26$
 $36 \bmod 26$
 $10 \quad (k)$

10) $c = (2-7) \bmod 26$
 $-5 \bmod 26$
 $21 \bmod 26$
 $21 \quad (v)$

11) $o = (14-7) \bmod 26$
 $7 \bmod 26$
 $33 \bmod 26$
 $7 \quad (h)$

12) $m = (12-7) \bmod 26$
 $5 \bmod 26$
 $31 \bmod 26$
 $5 \quad (f)$

$\{ \equiv \}$ congruent
Two int a and b are said to be congruent if
 $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$
"Rough 'n' Fair"

Mathematics of Cryptography

Modular Arithmetic and Congruence

($+, -, \times, \div$)
any $N = qM + R$ remainder
 q & R are int

1) $-50 \bmod 10$ 2) $-51 \bmod 10$
 $-50 = -5 \times 10 + R$ $-51 = -6 \times 10 + R$
 $-50 + 50 = R$ $-51 + 60 = R$
 $R = 0$ $R = 9$

3) $60200 \bmod 11$ 4) $2 \times 4 \bmod 11$
 $60200 \div 11$ $8 \div 11$
 $= 8$ 8

5) $73 \equiv 4 \pmod{23}$ 6) $-10 \bmod 3$
 $73 \div 23 = 4 \div 23$ $-10 = q \times 3 + R$
 $4 = 4$ $-10 = -4 \times 3 + R$
 $R = 2$

Congruent \equiv

7) $113 \bmod 24$ 8) $-29 \bmod 7$
 $113 \div 24$ $-29 = q \times 7 + R$
 $= 7$ $-29 = -5 \times 7 + R$
 $R = 6$

9) $3 \equiv 3 \pmod{17}$
 $3 \div 17 = 3 \div 17$
 $3 = 3$ congruent \equiv

How to find modulus of -ve number
 $(Mod\ (2))$
Ex - $N \equiv 0 \pmod{m}$

Method

$$N = qM + R$$

N or M → int no

\rightarrow remainder

$q \rightarrow$ we have to choose q such that
we get more or equal \rightarrow no
Thus n .

Evaluate

$$(200 - 30) \bmod 11 = (2^4) \bmod 11$$

$$-101 \bmod 11 \quad 8 \bmod 11$$

$$\text{and } 1) \text{ and } 1) - 101 + 110 = R$$

$$-4) \text{ and } 11 \quad R = 9 \quad 8$$

$$g(1) \neq R$$

$$R = 9.$$

$$2) (200 + 301) \bmod 11 = (2+4) \bmod 11$$

$$50 \bmod 11 = 8 \bmod 11$$

$$6 \neq 8$$

3) 123 + 62 Mind 1

$\int 123 \cdot 1.12 + 62 \cdot 1.12) \cdot 1.12$

(3 * 2) - 1.12

5-1-12
TBS Ag

Usage of Modular Arithmetic

Modular arithmetic is very well understood in terms of algorithms for various basic operations. That is one of the reason why we use finite fields (AES) in symmetric key cryptography. Cryptography requires hard problems. Some problems become hard with modular arithmetic.

For eg algorithms are easy to compute
are all integers but can become hard
to compute when you introduce a
modular reduction.

Similarly with finding roots

Mod arithmetic is the central mathematical concept in cryptography. Almost any cipher from the Caesar cipher to the RSA cipher use it.

There are two types of mod

- The mod function
 - The (mod) congruence

Modular arithmetic is the branch of arithmetic mathematics related with the 'mod' functionality. Basically, modular arithmetic is related with computation of 'mod' of expressions

Expressions may have digits and computational symbols of addition, subtraction, multiplication, division or any other. Here we will discuss briefly about all modular arithmetic operations.

Congruent Modulo/ congruence Cryptography

Congruent numbers

Integers that leave the same remainder when divided by the modulus n are somehow similar, however not identical. Such numbers are called 'congruent'. For instance 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12.

To show that two integers are congruent we use the congruence operator (\equiv)

For eg we write

$$(a \bmod n) \equiv (b \bmod n)$$

This written as

$$a \equiv (b \bmod n) \text{ or } b \equiv (a \bmod n)$$

Example

$$73 \equiv 4 \pmod{23}$$

$$73 \bmod 23 \equiv 4 \bmod 23$$

- $2 \equiv 12 \pmod{10}$

$$2 \bmod 10 \equiv 12 \bmod 10$$

- $13 \equiv 11 \pmod{5}$

$$13 \bmod 5 \equiv 11 \bmod 5$$

- $13 \equiv 15 \pmod{5}$

$$\text{No } 13 \bmod 5 \neq 15 \bmod 5$$

Set of Residues

The modulo operation creates a set which is modular arithmetic is referred to as the set of least residues mod n or \mathbb{Z}_n .

Some \mathbb{Z}_n sets

$$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, (n-1)\}$$

$$\mathbb{Z}_3 = \{0, 1, 2\} \quad \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

which of the following is true?

- 1) $3 \equiv 3 \pmod{17}$ True
- 2) $3 \equiv -3 \pmod{17}$ False
- 3) $172 \equiv 177 \pmod{5}$ True
- 4) $-13 \equiv 13 \pmod{26}$ True

Modular Arithmetic Operation Properties

First Property

$$(a+b) \pmod{n} = [(a \pmod{n}) + (b \pmod{n})] \pmod{n}$$

Second Property

$$(a-b) \pmod{n} = [(a \pmod{n}) - (b \pmod{n})] \pmod{n}$$

Third Property

$$(a \times b) \pmod{n} = [(a \pmod{n}) \times (b \pmod{n})] \pmod{n}$$

→ First Property

$$\text{Let } A=14 \quad B=17 \quad C=5$$

$$\begin{aligned} L.H.S \quad (A+B) \pmod{C} &= (14+17) \pmod{5} \\ &= 31 \pmod{5} \\ &= 1 \end{aligned}$$

$$\begin{aligned} R.H.S \quad &[(a \pmod{c}) + (b \pmod{c})] \pmod{c} \\ &[(14 \pmod{5}) + (17 \pmod{5})] \pmod{5} \\ &(4+2) \pmod{5} \\ &6 \pmod{5} \\ &1 \\ \therefore L.H.S &= R.H.S \end{aligned}$$

Same goes for Second & Third Property

- Q) Determine whether 17 is congruent to 5 modulo 6, and whether 24 and 14 are congruent modulo 6

$$\begin{aligned} 17 &\equiv 5 \pmod{6} & 17-5 &= 12 \\ 17 \pmod{6} &\equiv 5 \pmod{6} & \text{Multiple of } 6 \\ 5 &\not\equiv 5 \end{aligned}$$

$$\begin{aligned} 24 &\equiv 14 \pmod{6} & 24-14 &= 10 \\ 24 \pmod{6} &\equiv 14 \pmod{6} & \text{Not a multiple of 6} \\ 0 &\not\equiv 2 \end{aligned}$$

Q) Evaluate

- | | |
|--------------------|--------------|
| 1) $100 \pmod{26}$ | 22 |
| 2) $26 \pmod{26}$ | 02 |
| 3) $13 \pmod{26}$ | 13 |
| 4) $-5 \pmod{26}$ | $-5+26 = 21$ |
| 5) $12 \pmod{26}$ | 12 |

Q) Solve

$$\begin{aligned} 1) \quad & 5+10 \bmod 26 \\ 2) \quad & 13-16 \bmod 26 \\ 3) \quad & 32+46 \bmod 26 \end{aligned}$$

$$\begin{array}{l} 15 \\ -16 \\ \hline 7 \\ 0 \end{array}$$

Q) Add 7 to 14 in 215

$$\begin{aligned} 7+14 & \bmod 15 \\ 21 & \bmod 15 \\ 6 \end{aligned}$$

Q) Subtract 11 from 7 in 213

$$\begin{aligned} 7-11 & \bmod 13 \\ (7 \bmod 13 - 11 \bmod 13) & \bmod 13 \\ (7-11) & \bmod 13 \\ -4 & \bmod 13 \\ -14+13 = R & \\ R = 9. \end{aligned}$$

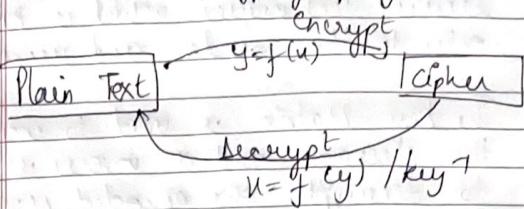
Q) Multiply 11 by 7 in 220

$$\begin{aligned} 11 \times 7 & \bmod 20 \\ 77 & \bmod 20 \\ 17 \end{aligned}$$

$$\begin{aligned} 7^2 \pmod{13} \\ 49 \bmod 13 \\ 10 \end{aligned}$$

#unit
DATE _____
PAGE _____
"Rough 'n' Fair"

Matrices in Cryptography



Q) $-13 \equiv 13 \pmod{26}$ check whether it is valid or invalid

$$-13 \equiv 13 \pmod{26}$$

$$-13 = -1 \times 26 + R \equiv 13$$

$$13 \equiv 13 \\ -13 \not\equiv 13 \pmod{26} \text{ - false they are congruent}$$

Q) One of the applications (important) of inverse of a square matrix is in Cryptography

Cryptography is an art of communication between two people by keeping the info not known to others. It is based upon two factors i.e
Encryption
Decryption

Encryption & Decryption requires a secret technique which is known only to the sender and receiver.

Note The key matrix is used to encrypt the message and its inverse is used to decrypt the encoded message. It is important that key matrix is kept secret between the message sender and receiver.

If the key matrix or its inverse is discovered that all the users, all hackers can easily decode the message.

$$\text{eg} \quad A = \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Message = "Welcome"
(W E L) (C O M) (E O O)

Uncoded matrix

$$[23, 5, 12]$$

Encoding matrix

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Coded message matrix

$$[45, -28, 23]$$

$$[8, 15, 13]$$

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$[46, -18, 3]$$

$$[5, 0, 0] \quad \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad [5, -5, 5]$$

$$\text{decoding matrix} = \frac{1}{|A|} \text{adj} A \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$

$$|A| = 1(0-0) - (-1)(0-0) + 1(0+1) \\ = 0 - 0 + 1 \\ = 1$$

Q Encrypt the message "COVID" using the encryption matrix

$$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

COV 1 DO

$$[3, 15, 22] \quad \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad [55, -18, 3]$$

$$[9, 4, 0] \quad \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad [17, -13, 9]$$

$$\text{decoding matrix} \quad \frac{1}{|A|} \text{adj} A \quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$