CRYPTOGRAPHY AND NETWORK SECURITY

MODULE-1 NOTES

I. Introduction to Computer Security:

- Computer security refers to the protection of computer systems, networks, and data from unauthorized access, misuse, modification, destruction, and service disruption.
- It ensures that information stored in computers and transmitted across networks remains protected against both accidental and intentional threats.
- As modern society increasingly relies on digital technologies for communication, business operations, education, healthcare, and governance, computer systems have become valuable targets for attackers.
- Computer security therefore aims to ensure that information resources are used only in authorized ways and remain dependable throughout their lifecycle.

Example: When you log in to your Gmail account, Google uses security mechanisms such as passwords, encryption, and login verification to prevent unauthorized users from accessing your emails. Without computer security, anyone could read or modify your private messages.

II. Need and Objective of computer Security

- The need for computer security arises because modern systems store large amounts of sensitive data and are constantly connected to the internet.
- Attackers attempt to steal personal information, financial details, business secrets, and government data.

- The main objectives of computer security are:

  1. To prevent unauthorized access
  2. To protect data from alteration
  3. To ensure systems remain operational

Example: Banks use computer security to protect customer account details and online transactions. If security is weak, attackers could transfer money illegally or steal credit card information.

III. CIA Triad (Confidentiality, Integrity, Availability)

The CIA Triad represents the three core principles of information security.

1. **Confidentiality** means that information is accessible only to authorized users. Encryption and authentication are commonly used to achieve confidentiality.

   Example: Password Protected files, without the particular password decryption of the File is not possible, it will stay encrypted.

2. **Integrity** ensures that data remains accurate and unaltered. Hash functions and digital signatures help detect changes.

   Example: HASH(SHA-256)

   Input: "hello"

   Hash: 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

   Input: "hell0"

   Hash: bdeddd433637173928fe7202b663157c9e1881c3e4da1d45e8fff8fb944a4868

   Although the two inputs differ by only one character, their hash values are entirely different. This property allows systems to quickly determine whether data has been altered, thereby ensuring integrity.

3. **Availability** ensures that systems and data are accessible whenever needed. Backup systems and protection against attacks support availability.

   Example: Movie ticket booking platforms must remain accessible even during heavy user traffic. They use multiple servers and backup systems so that if one server fails, another continues the service. This ensures users can book tickets without interruption.

IV. Threats, Vulnerabilities, and Risks

- A **threat** is any potential cause of harm to a system. A **vulnerability** is a weakness that can be exploited. **Risk** is the possibility that a threat will exploit a vulnerability and cause damage.
- Threats include hackers, malware, natural disasters, and insider misuse. Vulnerabilities include weak passwords, outdated software, and misconfigured servers.

Example: Using an old version of Windows without updates is a vulnerability. A hacker exploiting this weakness is a threat. If the system gets infected, the damage caused represents risk

V. Types of Security

1. **Physical Security** protects hardware from theft and damage.
2. **Network Security** protects data traveling over networks.
3. **Host Security** protects individual computers.
4. **Application Security** protects software applications.
5. **Data Security** protects stored and transmitted information.

   Example:
   A company locks its server room (physical), uses firewalls (network), installs antivirus (host), tests its website code (application), and encrypts databases (data).

VI. Security Policies and Security Models

- A security policy is a document that defines rules and responsibilities for protecting information. Security models provide theoretical frameworks for implementing policies.
- Policies define what users can and cannot do. Models help enforce those rules technically.

Example:

A college policy may state that students cannot access faculty salary records. The system enforces this using access control mechanisms.

VII. User Authentication and Authorization

- Authentication verifies who a user is. Authorization determines what the user can access.
- Authentication methods include passwords, biometrics, and smart cards. Authorization assigns permissions after identity is confirmed.

Example:

Logging into a university portal verifies your identity (authentication). Viewing only your marks and not others' marks is authorization.

VIII. Malware and Insider Threats

- Malware includes viruses, worms, Trojans, spyware, and ransomware.
- Insider threats come from employees misusing access.

Example:

An employee copying company data to a USB drive and selling it is an insider threat.

IX. Active and Passive Attacks

- Security attacks can be broadly classified into **passive attacks** and **active attacks** based on whether the attacker only observes information or actually interferes with the system.
- A **passive attack** occurs when an attacker secretly monitors or listens to communication without altering the data. The main objective of a passive attack is to **gain information**, such as usernames, passwords, or confidential messages, while remaining undetected.
- An **active attack**, on the other hand, involves **modifying, deleting, or disrupting data or services**. In this type of attack, the attacker directly interferes with the system's normal operation.

X. Denial of Service (DoS)

- A Denial of Service attack occurs when an attacker overwhelms a system or server with a large number of requests, making it unable to respond to legitimate users.
- **Example:**
  An attacker sends excessive traffic to a website, causing it to become slow or unavailable.

XI. Distributed Denial of Service (DDoS)

- A Distributed Denial of Service attack is similar to DoS, but the traffic is generated from many compromised computers at the same time, making the attack more powerful and harder to stop.
- **Example:**
  Thousands of infected computers flood an e-commerce website during a sale, causing the site to crash.

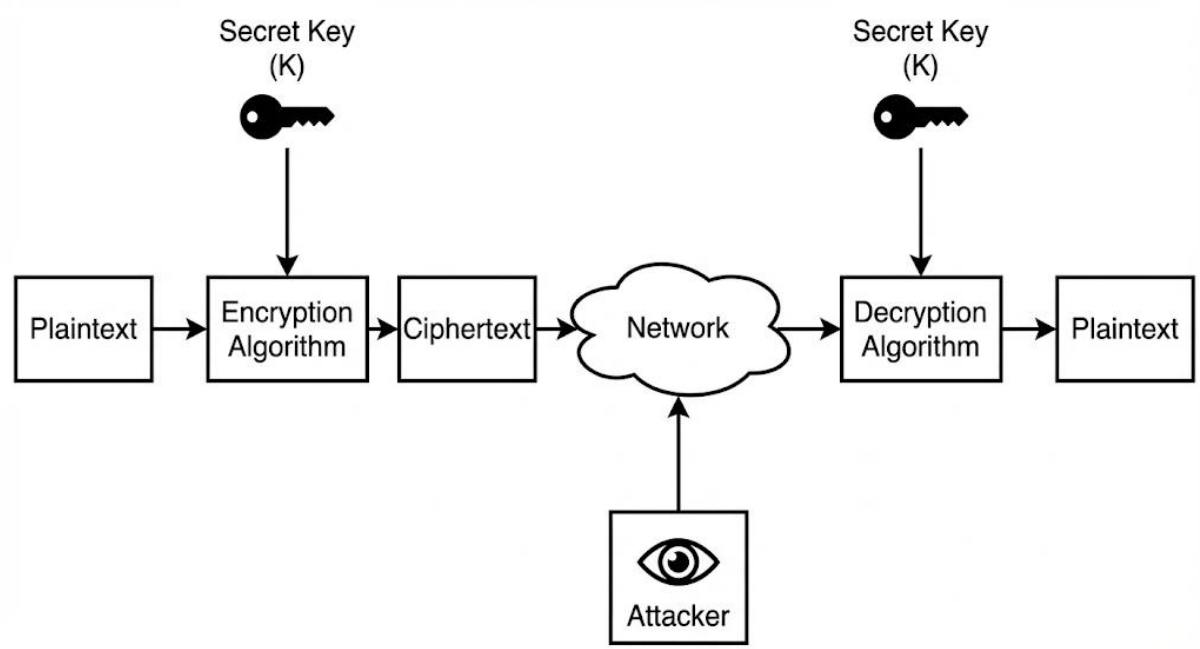
Network Security Model

The Network Security Model explains how secure communication takes place between a sender and a receiver over an insecure network. It shows how encryption, decryption, keys, and security mechanisms are used to protect data from attackers.

The main goal of the model is to ensure that information remains confidential, authentic, and unchanged during transmission.

Objectives of Network Security Model

- Protect data from unauthorized access
- Ensure confidentiality and integrity
- Provide authentication between sender and receiver
- Prevent attackers from understanding transmitted data



Working of Network Security Model

1. Sender converts plaintext into ciphertext using an encryption algorithm and a secret key.
2. Ciphertext is transmitted over the communication channel.
3. Receiver applies the decryption algorithm with the secret key.
4. Original plaintext is recovered.

Important Parameters

1. Plaintext

The original message or data that needs protection.

2. Encryption Algorithm

A mathematical technique used to convert plaintext into ciphertext.

3. Ciphertext

The encrypted form of plaintext that appears meaningless.

4. Decryption Algorithm

The reverse process of encryption that converts ciphertext back into plaintext.

5. Key

A secret value used during encryption and decryption.
Security depends mainly on the secrecy of the key.

6. Communication Channel

The medium used to transmit ciphertext.
It is assumed to be insecure.

7. Attacker (Intruder)

An unauthorized entity attempting to access or modify data.

Security Services Provided

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Advantages of Network Security Model

- Easy understanding of secure communication
- Helps in designing security systems
- Identifies possible attack points

Limitations of Network Security Model

- Conceptual model only
- Does not specify algorithms

Classical Encryption Techniques

Classical encryption techniques are early cryptographic methods used to protect information before the development of modern computer-based cryptography. These techniques rely on simple mathematical operations and manual procedures. Although they are not secure by modern standards, classical ciphers form the foundation of cryptography and help in understanding how encryption works.

Classical ciphers have two categories: **Substitution techniques** and **Transposition techniques**.

Substitution Techniques

Substitution techniques are encryption methods in which each element of the plaintext (letter, symbol, or group of letters) is replaced with another symbol according to a fixed rule.

1. Caesar Cipher (Shift Cipher).

- The Caesar cipher is a substitution cipher in which each letter in the plaintext is replaced by a letter that is a fixed number of positions ahead in the alphabet.
- The Caesar cipher is easy to implement but not secure because it has only 25 possible keys.
- Plaintext letters are first mapped to index values starting from 0 (A = 0, B = 1, ..., Z = 25). Based on this index value, the key (shift) is applied to generate the corresponding ciphertext letter.

Encryption Formula

$$C = (P + K) \bmod 26$$

Where:

C = Ciphertext letter

P = Plaintext letter

K = Key (shift value)

Decryption Formula

$$P = (C - K) \bmod 26$$

Example 1: Encryption

PLAINTEXT: NOTHING

KEY = 3

Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

1 N ⟶ Q (13 + 3) mod 26 = 16

2 O ⟶ R (14 + 3) mod 26 = 17

3 T ⟶ W (19 + 3) mod 26 = 22

4 H ⟶ K (7 + 3) mod 26 = 10

5 I ⟶ L (8 + 3) mod 26 = 11

6 N ⟶ Q (13 + 3) mod 26 = 16

7 G ⟶ J (6 + 3) mod 26 = 9

Output:

Plain Text: “NOTHING” → CIPHER TEXT: “QRWKLQJ”

Decryption: Key=3

Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

1 Q ⟶ N (16 - 3) mod 26 = 13

2 R ⟶ O (17 - 3) mod 26 = 14

3 W ⟶ T (22 - 3) mod 26 = 19

4 K ⟶ H (10 - 3) mod 26 = 7

5 L ⟶ I (11 - 3) mod 26 = 8

6 Q ⟶ N (16 - 3) mod 26 = 13

7 J ⟶ G (9 - 3) mod 26 = 6

Output:

Cipher text: “QRWKLQJ” → Plain Text: “NOTHING”

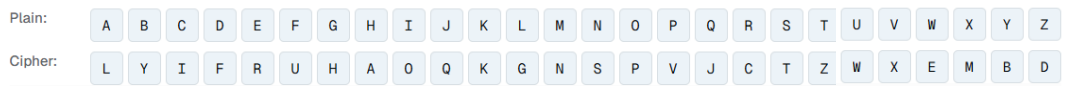
2. Mono Alphabetic Cipher

- The Monoalphabetic cipher is a substitution cipher in which each plaintext letter is replaced by a fixed corresponding ciphertext letter using a substitution table.
- • The same substitution mapping is used throughout the entire message.
- • The Monoalphabetic cipher is more secure than the Caesar cipher but is still vulnerable to frequency analysis attacks.
- • Plaintext letters are first mapped to index values starting from 0 (A = 0, B = 1, ..., Z = 25). Each plaintext letter is substituted with its corresponding ciphertext letter based on the substitution table.
- **Encryption Formula**
  a. $C = f(P)$

  Where:
  C = Ciphertext letter
  P = Plaintext letter
  f = Substitution function
- **Decryption Formula**
  a. $P = f^{-1}(C)$

  Where:
  f^{-1}= Inverse substitution function

Example:
Encryption:
Substitution key= LYIFRUHAOQKGNSPVJCTZWXEMBD P = NOTHING



Output:

Plaintext: NOTHING Ciphertext: SPZAOSH

3. Playfair Cipher

- The Playfair cipher is a digraph substitution cipher in which pairs of plaintext letters are encrypted instead of single letters.
- It uses a 5 × 5 matrix constructed using a keyword to perform encryption and decryption.
- The letters I and J are usually treated as the same letter and placed in a single cell.
- Plaintext is divided into letter pairs. If a pair contains identical letters, an X is inserted between them. If the last pair is incomplete, X is added.
- The Playfair cipher is more secure than simple substitution ciphers because it hides single-letter frequency.

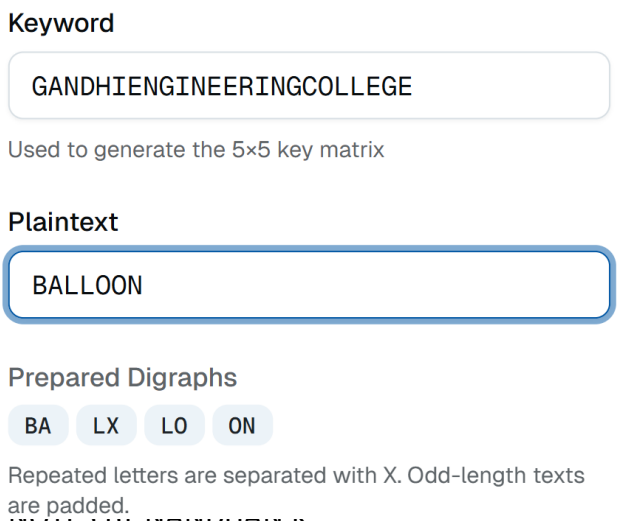
Encryption Rules

1. If both letters are in the same row, replace each letter with the letter to its right.
2. If both letters are in the same column, replace each letter with the letter below it.
3. If the letters form a rectangle, replace each letter with the letter in the same row and the column of the other letter.

Decryption Rules

1. If both letters are in the same row, replace each letter with the letter to its left.
2. If both letters are in the same column, replace each letter with the letter above it.
3. If the letters form a rectangle, replace each letter with the letter in the same row and the column of the other letter.

Example:



5×5 Key Matrix

G	A	N	D	H
I	E	R	C	O
L	B	F	K	M
P	Q	S	T	U
V	W	X	Y	Z

Steps:

Step 1 — Same Column

BA ⟶ QE

(3,2) + (1,2)

Step 2 — Rectangle

LX ⟶ FV

(3,1) + (5,3)

Step 3 — Rectangle

LO ⟶ MI

(3,1) + (2,5)

Step 4 — Rectangle

ON ⟶ RH

(2,5) + (1,3)

Output:

```
BA LX LO ON
```

```
QEFVMIRH
```

4. Hill Cipher

- The Hill cipher is a polygraphic substitution cipher that encrypts blocks of letters using matrix multiplication.
- • It uses linear algebra and a key matrix for encryption and decryption.
- • Plaintext letters are converted into numerical values (A = 0, B = 1, ..., Z = 25).
- • The plaintext is divided into fixed-size blocks based on the order of the key matrix.
- • The Hill cipher provides better security than simple substitution ciphers because it encrypts multiple letters at a time.

Encryption Formula

$$C = (K \times P) \bmod 26$$

Where:

C = Ciphertext vector

K = Key matrix

P = Plaintext vector

Determinant of K matrix

$$\det(K) = ad - bc \text{(for 2×2 matrix)}$$

GCD Verification So That Decryption is Possible or Not

GCD (det(k) mod 26 ,26)

If GCD is 1 then Decryption is possible, else it is impossible then we have to choose another key (K).

Decryption Formula

$$P = (K^{-1} \times C) \bmod 26$$

Where:

K^{-1}= Inverse of key matrix modulo 26

Determinant of Key Matrix

$$\det(K) = ad - bc \text{(for 2×2 matrix)}$$

If,

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

Adjoint of Key Matrix

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

Inverse of Key Matrix

$$K^{-1} = (\det(K)^{-1} \times \text{adj}(K)) \text{mod } 26$$

Where:

$$\det(K)^{-1} \times \det(K) \equiv 1 (\text{mod} 26)$$

Conditions for Key Matrix

- The determinant of the key matrix must be relatively prime to 26.
- Only then the inverse of the matrix exists.

Advantages

- Encrypts blocks of letters
- More secure than monoalphabetic cipher

Limitations

- Key matrix must be invertible
- Vulnerable to known-plaintext attack

Example:

Plain Text: “APPLE”

Step 1 — Check if Key is Valid

$$\det(K) = (3)(5) - (3)(2) = 15 - 6 = 9$$
$$\gcd(9,26) = 1$$

✓ Key is invertible → encryption & decryption possible.

Step 2 — Convert Plaintext to Numbers

A P P L E

0 15 15 11 4

Group into pairs:

$(0,15), (15,11), (4,X)$

Since length is odd → pad with X (23)

$(0,15), (15,11), (4,X)$

Step 3 — Encrypt Each Pair

Formula:

$$C = K \times P (\text{mod} 26)$$

Block 1: (0,15)

$$\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}0\\15\end{bmatrix}=\begin{bmatrix}45\\75\end{bmatrix}$$

= [45 mod 26, 75 mod 26] ➔ (19,23)

Encrypted Text: T X

Block 2: (15,11)

$$\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}15\\11\end{bmatrix}=\begin{bmatrix}78\\85\end{bmatrix}$$

= [78 mod 26, 85 mod 26] ➔ (0,7)

Encrypted Text: A H

Block 3: (4,23)

$$\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}\begin{bmatrix}4\\23\end{bmatrix}=\begin{bmatrix}81\\123\end{bmatrix}$$

= [81 mod 26, 123 mod 26] ➔ (3, 19)

Encrypted Text: D T

Plaintext = “APPLE” Ciphertext= “TXAHDT”

Decryption:

$$K=\begin{bmatrix}3 & 3\\2 & 5\end{bmatrix}$$

Step 1 — Compute Determinant

$$\det(K) = (3)(5) - (3)(2) = 15 - 6 = 9$$

$$\gcd(9,26) = 1$$

So an inverse exists.

Step 2 — Find Modular Inverse of det(k) (mod 26)

We need x such that:

$$9x \equiv 1(\text{mod}26)$$

Try values:

$$9 \times 3 = 27 \equiv 1(\text{mod}26)$$

So:

$$9^{-1} mod 26 = 3$$

$$\boxed{d^{-1} = 3}$$

Step 3 — Compute Inverse Matrix

For 2×2 matrix:

$$K^{-1} = d^{-1}\, adj(k)\, mod 26$$

For:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Adjugate:

$$\text{Adj(k)} = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

Here if we want we can reduce Adj(k) with mod 26 so we can reduce -ve values Else it will be applied directly while finding the K^{-1}.

Multiply by inverse of determinant (3):

$$K^{-1} = 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} mod\ 26 = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix}$$

Convert negatives mod 26:

$$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Step 4 — Convert Ciphertext to Numbers

T X A H D T

19 23 0 7 3 19

Group into pairs:

(19,23) (0,7) (3,19)

Step 5 — Decrypt Each Pair

Formula:

$$P = K^{-1} \times C (\text{mod} 26)$$

Block 1: (19,23)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 23 \end{bmatrix} mod\ 26 = \begin{bmatrix} 676 \\ 587 \end{bmatrix} mod\ 26$$

(676 mod 26, 587 mod 26) = (0,15) ➔ A P

Block 2: (0,7)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 7 \end{bmatrix} = \begin{bmatrix} 119 \\ 63 \end{bmatrix}$$

(119 mod 26, 63 mod 26) = (15, 11) ➔ P L

Block 3: (3,19)

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 19 \end{bmatrix} = \begin{bmatrix} 368 \\ 231 \end{bmatrix}$$

(368 mod 26, 231 mod 26) = (4, 23) ➔ E X

Step 6 — Final Plaintext

AP P L E X

Remove padding X:

APPLE

Cipher text = “TXAHDT” → Plaintext = “APPLE”

5. Vigenère Cipher (Polyalphabetic Cipher)

The Vigenère cipher is a **polyalphabetic substitution cipher** that encrypts letters using multiple Caesar shifts based on a keyword.

• It uses a repeating **key** to determine shifting values.

• Each plaintext letter is encrypted using a different alphabet.

• Plaintext letters are converted into numerical values (A = 0, B = 1, ..., Z = 25).

• The key is repeated until it matches the length of the plaintext.

• The Vigenère cipher is more secure than monoalphabetic ciphers because it uses multiple substitution alphabets.

Encryption Formula

$$C_i = (P_i + K_i) mod 26$$

Where:
C_i = Ciphertext letter value
P_i = Plaintext letter value
K_i = Key letter value

Decryption Formula

$$P_i = (C_i - K_i) mod 26$$

Where:
P_i = Plaintext letter value
C_i = Ciphertext letter value
K_i = Key letter value

Key Repetition Rule

The keyword is repeated until it matches the length of the plaintext.

Example:

Plaintext: WEAREDISCOVEREDSAVEYOURSELF "length = 27"
Key: DECEPTIVEDECEPTIVEDECEPTIVE "Length = 9 x 3 = 27"

Character Mapping

A = 0, B = 1, C = 2, ..., Z = 25

Working Principle

• Convert plaintext letters into numbers.

• Convert key letters into numbers.

• Add corresponding values modulo 26 to encrypt.

• Subtract corresponding key values modulo 26 to decrypt.

• Convert resulting numbers back to letters.

Conditions for Correct Decryption

• Sender and receiver must use the **same key**.
• Key must be repeated correctly.

Advantages

• Polyalphabetic encryption
• More secure than Caesar cipher
• Resists simple frequency analysis

Limitations

• Repeating keys can be exploited
• Vulnerable to Kasiski Examination
• Not secure against modern cryptanalysis

Example:
Plain text = WEAREDISCOVEREDSAVEYOURSELF

Cipher text =DECEPTIVE

Plaintext Characters

W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A
V	E	Y	O	U	R	S	E	L	F							

Key Sequence (Repeating)

D	E	C	E	P	T	I	V	E	D	E	C	E	P	T	I	V
E	D	E	C	E	P	T	I	V	E							

Encryption Steps:

W + D = Z	22	+3	=25
E + E = I	4	+4	=8
A + C = C	0	+2	=2
R + E = V	17	+4	=21
E + P = T	4	+15	=19

Till…..

R + P = G	17	+15	=6
S + T = L	18	+19	=11
E + I = M	4	+8	=12
L + V = G	11	+21	=6
F + E = J	5	+4	=9

Ciphertext

```
ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

TRANSPOSITION CIPHERS

Rail Fence Cipher

The Rail Fence Cipher is a **transposition cipher** that encrypts plaintext by writing it in a zigzag pattern across multiple rails and then reading row by row.

- It rearranges the positions of letters rather than substituting them.
- Characters are written diagonally in a zigzag form.
- The number of rails acts as the key.
- It is one of the simplest classical transposition ciphers.

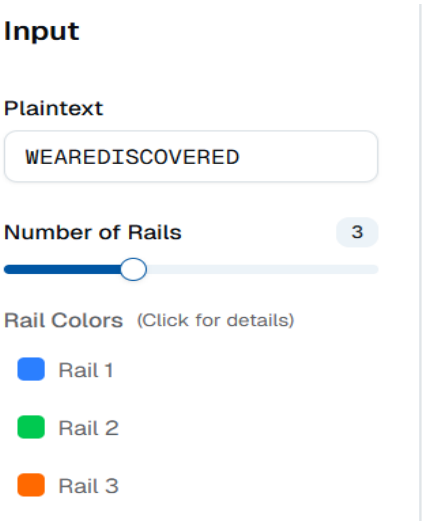
Encryption Procedure

1. Choose the number of rails (key).
2. Write the plaintext in zigzag form across the rails.
3. Read the letters row-wise to obtain the ciphertext.

Decryption Procedure

1. Create a zigzag pattern using the number of rails.
2. Place ciphertext letters row-wise into the pattern.
3. Read letters diagonally in zigzag order to recover plaintext.

Example:



Output

Plaintext (Input)

```
WEAREDISCOVERED
```

Ciphertext (Row-wise reading)

```
WECRERDSOEEAIVD
```

Columnar Transposition Cipher

The Columnar Transposition Cipher encrypts plaintext by writing it into rows under a keyword and then reading columns in a specific order.

• It rearranges letter positions without changing the letters themselves.

• The order of columns is determined by the alphabetical order of the key letters.

• It provides better security than simple rail fence cipher.

Encryption Procedure

1. Choose a keyword.
2. Number the letters of the keyword according to alphabetical order.
3. Write plaintext row-wise beneath the keyword.
4. Read columns according to the numerical order of the key.

Decryption Procedure

1. Determine the number of columns from the key length.
2. Fill columns based on key order using ciphertext.
3. Read the table row-wise to obtain plaintext.

Example:

Input

Plaintext

WEAREDISCOVERED

Numeric Key

4231

Each digit represents column reading order

Column Reading Order (Click for details)

1 2 3 4

1 2 3 4

Columnar Grid

Row	Key: 4 Read #4	Key: 2 Read #2	Key: 3 Read #3	Key: 1 Read #1
1	W	E	A	R
2	E	D	I	S
3	C	O	V	E
4	R	E	D	X

Column-wise Extraction (Click any column for details)

#1 1	#2 2	#3 3	#4 4
R	E	A	W
S	D	I	E
E	O	V	C
X	E	D	R

Output

Plaintext (Row-wise fill)

WEAREDISCOVEREDX

Ciphertext (Column-wise read)

RSEXEDOEAIVDWECR

Steganography (Information Hiding Technique)

Steganography is the art of **hiding secret information inside another innocent-looking medium** such that the existence of the message itself is concealed.

• Unlike cryptography, steganography hides the **presence** of communication.

• The secret message is embedded inside a cover object such as image, audio, video, or text.

• The receiver extracts the hidden data using a secret key or extraction algorithm.

• Used as a complementary technique to cryptography.

Basic Steganography Model

$$\text{Stego Object} = \text{Cover Object} + \text{Hidden Message} + \text{Key}$$

Terminology

Cover Object → Original file (image, audio, text, video)

Secret Message → Data to be hidden

Stego Object → File after embedding secret data

Stego Key → Key used for embedding and extraction

Embedding Process

1. Select cover object
2. Select secret message
3. Embed message using steganographic algorithm
4. Generate stego object

Extraction Process

1. Receive stego object
2. Apply extraction algorithm using key
3. Recover hidden message

Types of Steganography

• Text , Image, Audio, Video, Network Steganography

Common Techniques

• Least Significant Bit (LSB) substitution
• Masking and filtering
• Discrete Cosine Transform (DCT)
• Spread Spectrum technique

Steganography vs Cryptography

Steganography	Cryptography
Hides existence of message	Hides content of message
Message invisible	Message visible but unreadable
Less suspicion	More suspicion
Often combined with crypto	Standalone technique

Advantages

• Conceals existence of data
• Useful for covert communication
• Can be combined with encryption

Limitations

• Limited data capacity
• Vulnerable to steganalysis
• File modification may destroy hidden data

Applications

• Secret communication
• Digital watermarking
• Copyright protection
• Military and intelligence systems

Perfect Security

Perfect security means that **even if an attacker intercepts the ciphertext, they learn absolutely nothing about the original message**.

In simple words:
Seeing the encrypted message does not help an attacker guess the plaintext in any way.

• The ciphertext gives zero useful information about the message
• Security does NOT depend on computing power
• Also called **information-theoretic security**

What Does Perfect Security Mean?

A cryptosystem has perfect security when:

The chance of guessing a plaintext remains the same before and after seeing the ciphertext.

This means the ciphertext does not change the attacker's knowledge.

Example:

One-Time Pad (OTP)

The One-Time Pad is the only cipher known to achieve perfect security.

Why One-Time Pad Is Perfectly Secure

• Every possible plaintext is equally likely
• No pattern exists in ciphertext
• Brute-force attacks are useless

How One-Time Pad Works

Encryption:

$$C = P \oplus K$$

Decryption:

$$P = C \oplus K$$

• P = Plaintext
• C = Ciphertext
• K = Random key
• $\oplus$ = XOR operation

Advantages

• Highest possible security
• Immune to cryptanalysis
• Independent of computing power

Limitations

• Impractical for most real systems
• Key management problem

Information Theory (in Cryptography)

Information Theory is the mathematical study of **information, data transmission, and uncertainty**.

In cryptography, it helps us measure **how much information is revealed by a ciphertext** and how secure an encryption system is.

Simply put:

Information Theory tells us how much an attacker can learn from encrypted data.

Why Information Theory Is Important

• Helps analyse secrecy of encryption systems
• Measures uncertainty and randomness
• Forms the basis for perfect security

Basic Terms

Information
Knowledge gained from a message.

Entropy
Measure of uncertainty or randomness.

Redundancy
Extra or predictable information in data.

Entropy (H)

Entropy measures **how unpredictable a message is**.

• High entropy → More randomness → More secure
• Low entropy → More patterns → Less secure

Example:

AAAAAA → Low entropy

X9@K2P → High entropy

Conditional Entropy

Conditional entropy measures how much uncertainty remains about the plaintext **after seeing the ciphertext**.

If conditional entropy is high → Good security.

Mutual Information

Mutual information measures **how much ciphertext reveals about plaintext**.

• For perfect security:
Mutual Information = 0

Meaning:

Ciphertext reveals nothing.

Product Cryptosystem

A Product Cryptosystem is created by **combining two or more simple cryptographic techniques** to build a stronger encryption system.

Instead of relying on a single cipher, multiple ciphers are applied in sequence.

Strength comes from combination.

Basic Idea

If:

Cipher A is weak
Cipher B is weak

Then:

Cipher A followed by Cipher B can be strong.

How It Works

Plaintext → Cipher 1 → Cipher 2 → Cipher 3 → Ciphertext

Each stage increases complexity.

Types of Combination

• Substitution + Substitution
• Substitution + Transposition
• Multiple rounds of substitution and transposition

Why Product Cryptosystems Are Used

• Single classical ciphers are easy to break
• Combination hides patterns
• Increases confusion and diffusion

Confusion and Diffusion

Confusion
Hides relationship between key and ciphertext.

Diffusion
Spreads plaintext structure across ciphertext.

Product cryptosystems aim to achieve both.

Modern Example (Conceptual)

Modern block ciphers like AES use:

• Multiple rounds
• Substitution
• Permutation
• Key mixing

They are product cryptosystems.

Cryptanalysis

Cryptanalysis is the art and science of breaking cryptographic systems.
It involves studying encryption methods to discover the hidden message or secret key without knowing the key.

Cryptanalysis helps identify weaknesses in cryptographic algorithms and plays an important role in improving security systems.

Objectives of Cryptanalysis

• Recover plaintext from ciphertext
• Discover the secret key
• Evaluate strength of cryptographic algorithms

Types of Cryptanalytic Attacks

1. **Ciphertext-Only Attack**

In this attack, the attacker has access only to ciphertext.
Using statistical analysis and patterns, the attacker attempts to guess plaintext or key.

2. **Known-Plaintext Attack**

The attacker knows some plaintext and its corresponding ciphertext.
This information is used to find the key or decrypt other messages.

3. **Chosen-Plaintext Attack**

The attacker can choose specific plaintexts and obtain their ciphertext.
This helps analyze how the encryption algorithm works.

4. **Chosen-Ciphertext Attack**

The attacker can choose ciphertexts and obtain their plaintext.
This attack is powerful against poorly designed encryption schemes.

5. **Brute-Force Attack**

The attacker tries all possible keys until the correct one is found.
Large key sizes make brute-force attacks impractical.

6. **Statistical Attack**

Uses frequency analysis and language patterns.
Commonly used against classical substitution ciphers.

Why Cryptanalysis Is Important

• Helps detect weaknesses
• Improves cryptographic design
• Validates security claims

Difference Between Cryptography and Cryptanalysis

Cryptography focuses on creating secure systems.
Cryptanalysis focuses on breaking them.

Advantages

• Strengthens security research
• Improves encryption standards.