Computer Security -II
IMP Questions

✅ Q1: Define the following terms

🌐 (1) Cyber Security

🔐 **Definition:**
Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from digital attacks.

📌 **In simple words:**
It keeps your data saf e from hackers, viruses, and other online threats 🚫

💡 **Real-life Example:**
Using antivirus software on your laptop to prevent hackers from stealing your files.

🔐 (2) Encryption

📄 **Definition:**
Encryption is th e process of converting plain data (plaintext) into a secret code (ciphertext) to prevent unauthorized access.

🔁 It uses algorithms to scramble data.

💡 **Real-life Example:**
WhatsApp messages a re encrypted, so only you and the receiver can read them 📱🔒

🚫 (3) Interruption

🛑 **Definition:**
Interruption is a type of security attack where system resources become unavailable or disrupted.

🔧 **Goal:** To stop or disturb normal services.

💡 **Example:**
A DDoS attac k floods a server with traffic so users can't access it.

📩 (4) Spam

🗑️ **Definition:**
Spam refers to unwanted, irrelevant, or inappropriate messages sent over the Internet, typically to a large number of users.

💡 **Example:**
You get 100 emails saying “You won a lottery!”—that’s spam 😑📧

💣 (5) System Abuse

⚠️ **Definition:**
System abuse is the misuse of computer systems for unauthorized or illegal purposes.

Example:
A company employee using office computers to mine cryptocurrency secretly ⛏️💻

🕵️ (6) Cryptanalysis

🔓 **Definition:**
Cryptanalysis is the study of analyzing information systems to break cryptographic security systems.

💣 **Goal:** Break encryption without having the key.

Example:
Trying to guess a password by analyzing encrypted files.

👃 (7) Sniffing Attack

👂 **Definition:**
A sniffing attack involves capturing data packets traveling over a network.

Goal: To steal sensitive information like usernames or passwords 🧠🎯

Example:
Using a tool like Wireshark to read login data sent over public Wi-Fi.

🛡️ (8) Cryptography

🔐 **Definition:**
Cryptography is the art of protecting information by transforming it into an unreadable format.

➡️ It’s used for **data privacy**, **authentication**, and **integrity**.

Real-life Example:
Bank websites use cryptography to secure online transactions 💳🔐

✔️ Q2: Short Questions

🔤 (1) Give full form of the following:

🔢 No.	🔠 Abbreviation	📜 Full Form
1️⃣	SMTP	Simple Mail Transfer Protocol
2️⃣	MIME	Multipurpose Internet Mail Extensions
3️⃣	SSL	Secure Sockets Layer
4️⃣	DES	Data Encryption Standard
5️⃣	AES	Advanced Encryption Standard
6️⃣	DSS	Digital Signature Standard
7️⃣	POP	Post Office Protocol
8️⃣	SET	Secure Electronic Transaction
9️⃣	STT	Secure Transaction Technology

🧠 Easy Tip: These are mostly **internet, email, or encryption-related terms** used in **cyber security & secure communication** 💬🔐

🔍 (2) List out causes of Vulnerability in system

🛠️ **System vulnerabilities** are weaknesses that hackers can exploit.
Here are the **main causes**:

➡️ **Weak Passwords** – Easy to guess (like “123456”)
Outdated Software – Not patched against known bugs
Unsecured Networks – Public Wi-Fi without protection
Lack of Encryption – Data transferred in plain text
Human Errors – Clicking on phishing links 🧑💻😫
Misconfiguration – Incorrect settings in system/software
➡️ **Infected Files** – Malware hidden in downloaded files

🔒 **Real-life example:**
Using the same password for all your accounts = high risk 🚨

🧑💻 (3) Who is a Hacker?

👨‍💻 **Definition:**
A hacker is someone who uses their technical knowledge to gain unauthorized access to computer systems or networks.

🧩 **Types of Hackers:**

- 👼 **White Hat:** Ethical hacker (helps fix issues)
- 😈 **Black Hat:** Illegal hacker (steals or damages data)
- 😐 **Grey Hat:** Hacks for fun or to show off flaws

💡 **Example:**
A white-hat hacker testing a website for weaknesses so it can be fixed.

⛔ (4) What is Interruption?

🛑 Already answered in **Q1 (3)** – but here's a recap:

👉 **Interruption** means a system or service becomes **unavailable** or is **stopped** due to an attack (like DDoS or hardware failure).

Real-life example:
A company website crashing during a big sale due to a traffic overload attack 🚦🧨

🔓 (5) What is System Vulnerability?

⚠️ **Definition:**
A system vulnerability is a weakness or flaw in the system's **design, implementation, or configuration** that can be **exploited** by threats.

📌 It is like a **hole in the wall** where intruders can sneak in!

Example:
An old version of Windows not updated with the latest security patch.

✔️ Q3 (1): List out and explain applications of Cryptography

🔐 **Cryptography** = Securing information by converting it into unreadable formats ✨

🌍 Applications of Cryptography:

📧 1. Secure Email Communication

➡️ Encrypts emails to prevent unauthorized access.

💌 **Example:** Gmail uses SSL/TLS to encrypt your email content.

💳 2. Online Banking & Payments

Protects your credit card and bank info during online transactions.

💰 **Example:** Websites with HTTPS use encryption for secure payments.

🔑 3. Password Storage

Stores passwords in encrypted (hashed) format to prevent misuse.

💡 **Example:** When you create a new password on Instagram, it's encrypted so not even Instagram can see it.

🔒 4. File & Disk Encryption

Secures sensitive files on your device or USB.

🗂️ **Example:** BitLocker (in Windows) encrypts your entire hard disk.

📱 5. Secure Messaging Apps

Messages are encrypted from sender to receiver (end-to-end encryption).

📲 **Example:** WhatsApp, Signal, Telegram.

🌐 6. VPN (Virtual Private Network)

Encrypts your internet traffic, hiding your browsing data from hackers.

🕵️ **Example:** Using NordVPN or ExpressVPN for private surfing.

🧾 7. Digital Signatures

Used to verify documents and sender's identity.

✍️ **Example:** e-Aadhar cards use digital signatures to validate identity in India 🇮🇳

Why it's important?

Cryptography protects our privacy, secures money transfers, prevents identity theft, and builds trust in digital communication 🔐🤝

✔️ Q3 (2): How many types of Security Attacks? Explain Modification in detail

🔐 Types of Security Attacks

Security attacks are actions that try to **break into, damage, or misuse** a computer system or network 💻⚠️
They are mainly divided into **2 categories**:

🗂️ A. Passive Attacks (🕵️ – Secret Watching)

➡️ **Definition:**
These attacks **do not affect** the system but try to **steal information**.

💡 **Examples:**

- 👂 **Eavesdropping:** Listening to network traffic.
- 🧐 **Traffic analysis:** Checking who is talking to whom and how often.

🎯 Goal: Steal or read confidential data without being noticed.

🛠️ B. Active Attacks (💣 – Real Damage)

Definition:
These attacks try to **change, damage, or destroy** system data or functions.

Examples:

- ✏️ **Modification Attack** (explained below)
- 🛑 **Denial of Service (DoS)**
- 👧💻 **Masquerade Attack**
- 🔁 **Replay Attack**

🎯 Goal: To **damage or disrupt** the system or **steal info** by force.

🔄 Detailed Explanation: MODIFICATION ATTACK

Definition:
In this attack, the hacker **modifies the original message or data** while it is being sent between sender and receiver.

🧠 Think of it like:
You send a message “Send ₹1000” ➡️ Hacker changes it to “Send ₹10,000” 😢💸

📦 How it works:

1. 🔁 Data is sent over the internet.
2. 🔓 Hacker intercepts the message.
3. 🛠️ He **modifies** the content (money amount, name, instructions).
4. 📤 The fake message is sent to the receiver.

💡 Real-life Example:

A hacker changes the bank account number in an email sent to a client, so money goes to the hacker's account instead of the company's 🏦➡️🦹

🔒 How to prevent it?

- Use **Encryption**
- Apply **Digital Signatures**
- Use **Secure Protocols (HTTPS, SSL/TLS)**

✔️ Q3 (3): What is System Abuse? Explain in detail with example

⚠️ Definition: System Abuse

🖥️ **System Abuse** means **misusing a computer system or network** in a way that violates its intended use, policies, or legal restrictions.

💣 It's like using someone else's car 🚗 to deliver illegal goods — you're using a tool for the wrong purpose.

🔍 Types of System Abuse

Let's break it down with real-life style explanations 🧠👇

🔓 1. Unauthorized Access
➡️ Accessing systems or files without permission.

🧑‍💻 Example:
A student hacks into a school's server to change exam marks 📚🚨

📂 2. Misuse of Resources
Using company computers for personal profit or entertainment.

💡 Example:
An employee mining cryptocurrency using office computers 💰 💼

✉️ 3. Sending Spam or Malware
Abusing email systems to send large-scale spam or viruses.

Example:
Sending thousands of fake emails with virus attachments 📬🦠

🎮 4. Personal Use of Organization Resources
Using internet, systems, or storage for personal gain.

Example:
Streaming Netflix all day on a work computer 😅🍿

🛑 5. Denial of Service (DoS)
➡️ Overloading systems intentionally to make them crash.

Example:
A disgruntled ex-employee floods a company's website with fake traffic to shut it down 🌐💥

🎯 Why it's dangerous?

- Can **harm organizations**
- Leads to **data theft**
- Causes **loss of trust**
- Wastes **money and time**

🛡️ How to prevent System Abuse?

✔️ Create strong **security policies**
Educate users (awareness programs)
Monitor usage (audit logs)
Use **antivirus, firewalls, and access control**

📌 **In simple words:**
System abuse = when a computer is used **for something wrong or illegal** 👦💻💣

✔️ Q3 (4): How to Prevent and Control Threats?

🚨 **Threats** in cybersecurity are anything that can **harm a system** — like hackers, viruses, or data theft 🦠

🛡️ How to Prevent & Control Threats:

Let's explore the **best ways** to protect your system 🧠👇

🔐 **1. Use Strong Passwords**
➡️ Mix of **capital, small, numbers & symbols**
Tip: Avoid using "password123" or birthdates!
🔁 Change them regularly!

2. Install Antivirus & Anti-Malware Software
Detects and removes viruses, worms, trojans
💡 Example: Quick Heal, Avast, Norton

🌐 **3. Use Firewalls**
Blocks **unauthorized network access**
🛑 Acts like a **security guard** between your system and the internet

🆙 **4. Keep Software Up to Date**
➡️ Regular updates fix **security bugs**
💡 Example: Update Windows, browsers, apps often

🔒 5. Enable Encryption

➡️ Converts data into unreadable format (ciphertext)

🔐 Even if stolen, hackers can't read it

🧑‍🏫 6. Educate Users

Train employees/students on **safe browsing**, avoiding suspicious links

---

🔎 7. Monitor Network Activities

Detects unusual or unauthorized activities

🧠 Use tools like Wireshark or Intrusion Detection Systems (IDS)

📂 8. Access Control

Only authorized users should access critical files

🔑 Give access based on roles (admin/user/guest)

💡 **Real-Life Analogy:**

Just like locking your home, installing cameras, and training family to be cautious — computers need layered protection too! 🏠💻🛡️

✔️ Q3 (5): Differentiate between Plain Text and Cipher Text

🆚 Feature	🔤 Plain Text	Cipher Text
📖 Meaning	Original readable message	Encrypted (unreadable) version of message
👀 Readable?	Yes, by humans and systems	No, looks like random characters
🎯 Purpose	To convey actual message	To hide the message from unauthorized users
🔄 Conversion Process	Written by sender	Created after encryption using an algorithm
🔒 Example	"Hello123"	"h8$#Jq92%" (after encryption)

📌 Real-life Example:

👉 **Plain Text:**

🧒 Rahul sends a message: *"I will pay ₹5000 tomorrow"*

Everyone can read it if intercepted 😬

👉 **Cipher Text:**
🔐 After encryption: *"XK&@tLq893!"*
Only someone with the **decryption key** can read it 🗝️

🎯 Why it matters?

🔒 Plain text is **not safe** for secret data
Cipher text **protects** your information during transmission

---

✔️ Q3 (6): Explain System Vulnerability and Write Causes of It

---

🧠 What is System Vulnerability?

🛠️ A **System Vulnerability** is a **weak point or flaw** in a computer system, software, or network that hackers can exploit to gain unauthorized access or cause damage 🔓💥

📌 **In Simple Words:**
It's like leaving your **main door open at night** — burglars (hackers) might walk right in! 🏚️🚪

⚠️ Common Examples of Vulnerabilities:

- Outdated software versions 👴
- Weak or reused passwords 😬
- Missing security patches 🧯
- Poorly coded applications 🧑‍💻

💣 Causes of System Vulnerabilities:

Let's look at why these weaknesses happen 🧠👇

🪛 1. Software Bugs
➡️ Programming errors create **loopholes**
💡 Hackers exploit these to crash systems or steal data

🕰️ **2. Outdated Systems**
➡️ No updates = No security patches
💣 Easy entry points for viruses and malware

🛑 **3. Weak Passwords**
Using simple or same passwords for all accounts
💡 Example: "admin123", "password" = Hacker's paradise 😅

📥 **4. Unchecked User Access**
Giving full system access to all users
🔓 Even junior users can accidentally or intentionally harm system data

🌐 **5. Poor Network Configuration**
Open ports, unprotected IP addresses
Invites network-based attacks like DDoS or sniffing

🧒🏫 **6. Lack of Awareness**
Untrained users clicking spammy links or downloading malicious files

🔁 **7. Third-Party Tools**
Using free, untrusted software from unknown sources 📦⚠️

🎯 **Bottom Line:**
A **vulnerability** is like a **hole in your system's shield** — it must be fixed to stay safe 🔧🛡️

✔️ Q3 (7): Explain Password Management with Its Challenges

🔐 What is Password Management?

📖 Password Management is the process of **creating, storing, updating, and protecting** passwords to keep systems secure 🛡️

📌 **Why is it important?**
💣 Passwords are the **first line of defense** — if weak or exposed, hackers can easily break in.

🔑 Good Practices in Password Management:

✔️ Use strong passwords
Avoid reusing passwords across platforms
Change passwords regularly
Use password managers (e.g., LastPass, Bitwarden)
Enable Two-Factor Authentication (2FA)

🧱 Challenges in Password Management:

😵 1. Human Memory Limits
➡️ Hard to remember complex, long passwords
💡 Example: Remembering `D$3Hfd7^K9!Z` for every account? 🧠❌

🔁 2. Password Reuse
People use the **same password** across multiple sites
💥 If one gets hacked, all are in danger!

📱 3. Phishing Attacks
Fake websites trick users into giving passwords
Looks like Gmail login, but it's fake 😨

💾 4. Unsecured Storage
Writing passwords in notebooks or saving in notepad
😬 Easy to steal if someone accesses the system

🧑‍💼 5. Lack of Awareness
Many users don’t know the importance of strong password habits
🛑 They use "123456" or "admin" without realizing the risk

🚧 6. No Use of Tools
➡️ Not using password managers, 2FA, or browser security tools

---

✔️ Solutions:

🔐 Use tools like **Bitwarden**, **1Password**, or **KeePass**
📲 Enable **2FA/MFA** for extra protection
🧠 Educate users on creating strong, memorable passwords using passphrases

---

📌 Example of Strong Password:
`MypetDog@2025RunsFast!` 🐶 — Easy to remember, hard to guess!

✔️ Q3 (8): Differentiate between Encryption and Decryption

🔐 What is Encryption & Decryption?

🔸 These are two **main processes in Cryptography** used to protect data during communication 🛰️

Think of it like **sending a secret letter** 📝 using a code, and the receiver **decodes** it to understand 💬

📊 Table: Difference between Encryption and Decryption

🆚 Feature	🔐 Encryption	🔓 Decryption
📖 Meaning	Converting plain text → unreadable form (ciphertext)	Converting ciphertext → readable form (plain text)
🎯 Purpose	To **protect** the data from unauthorized access	To **understand** the original data
🔄 Performed By	Sender (before sending data)	Receiver (after receiving data)
🔑 Uses Key?	Yes – uses **encryption key**	Yes – uses **decryption key**
🔒 Output Example	“Hello” → “8@#kL29$”	“8@#kL29$” → “Hello”

💡 Real-life Analogy:

📨 **Encryption:** Locking your message in a box with a key 🗝️
📬 **Decryption:** Unlocking the box on the other side with the correct key

Summary:

- **Encryption**: Hides your message 😶🌫️
- **Decryption**: Reveals it back 📜
  👉 Both are essential to protect your data in digital communication

✔️ Q3 (9): What is Plain Text? Explain with Example

🔤 Definition: Plain Text

➡️ **Plain Text** is the **original, readable form** of data or message that is not encrypted.

🧒🏫 It is the message **before encryption** or **after decryption**

💡 Simple Example:

📩 You want to send:
Plain text: "Meet me at 10 PM"

🛡️ After encryption, it becomes:
Ciphertext: "Z4$#kJ1^%k@!"

📤 This encrypted text is sent over the internet
Receiver decrypts it back to get the **original plain text**

🧠 Real-Life Analogy:

📝 **Plain Text** = Writing your secret on a **postcard** (anyone can read it)
🔐 Cipher Text = **Locking it in a coded box** (only someone with the key can read)

📌 Important Points:

- It's **human-readable** and understandable
- It's **NOT secure** when sent directly over the internet
- Should always be encrypted before transmission

✔️ Q3 (10): Differentiate Between Encryption and Decryption

> (Already explained in the previous message, but here's a fresh, quick recap with the same rich formatting!) 🧠👇

🔐 What is Encryption & Decryption?

➡️ These are two **core functions of Cryptography** used to **protect sensitive data** while it is transmitted or stored 💾🔐

📊 Table: Difference between Encryption and Decryption

🔍 Feature	Encryption	🔓 Decryption
✔️ Definition	Converts **Plain Text → Cipher Text**	Converts **Cipher Text → Plain Text**
🎯 Goal	To **hide the original message** from outsiders	To **reveal the hidden message** to intended user
🧑‍💻 Used By	Sender of the message	Receiver of the message
🛠️ Process	Uses an **encryption key or algorithm**	Uses a **decryption key or algorithm**
🗝️ Example	“Hello” → “9H#k^7w”	“9H#k^7w” → “Hello”

💬 **Analogy:**

- **Encryption** = Locking your diary with a secret lock 🔒
- **Decryption** = Unlocking it with the right key 🗝️

✔️ Both are **equally important** to ensure **data confidentiality** in digital communication 🛡️

✔️ Q3 (11): Define Cryptography. Discuss the Types of Cryptography in Detail

🧠 What is Cryptography?

📖 **Cryptography** is the science of **writing and solving codes** to protect information from unauthorized access or alteration 🧑‍💻

> 👉 It is used to **convert readable data (plain text) into coded format (cipher text)** to prevent others from reading it 📜→🔒

🎯 Main Purpose of Cryptography:

- ✔️ Data Privacy (No one else can read it)
- Authentication (Data comes from the right person)
- Data Integrity (No tampering during transmission)
- Non-repudiation (Sender can't deny sending it)

🔍 Types of Cryptography:

1️⃣ Symmetric Key Cryptography (Private Key) 🔑🔁

- Both sender and receiver use **the same key** for encryption & decryption.
- Fast and simple 💨
- But: If the key is stolen, everything is exposed ❗

🧠 **Example:**

> You and your friend both know the lock code "1234" for a locker. You lock it, they unlock it with the same code.

💬 **Used In:** AES, DES, RC4, etc.

2️⃣ Asymmetric Key Cryptography (Public Key) 🗝️🔐

- Uses **two different keys**:
  🔑 **Public key** – for encryption
  🗝️ **Private key** – for decryption
- More secure but slower 🐢

🧠 **Example:**

> You share your **public key** with everyone to receive messages, but only you can read them using your **private key**

💬 **Used In:** RSA, ECC

3️⃣ Hash Functions (One-Way Encryption) 🧩❌🔁

- No key involved
- Converts data into a fixed-size **hash value** (irreversible)

- Mainly used for **data integrity** and **password security**

🧠 **Example:**

Hashing "MyPassword123" becomes "9c5a8a2c4b1e..." (can't be reversed back)

💬 **Used In:** MD5, SHA-256, bcrypt

📊 Table Summary:

🔍 Type	🔑 Keys Used	🔁 Direction	🔐 Example Algorithms
Symmetric Key	Same key for both	Two-way	AES, DES
Asymmetric Key	Public & Private key	Two-way	RSA, ECC
Hash Functions	No key (one-way only)	One-way (irreversible)	SHA-256, MD5

✔️ Real-Life Usage of Cryptography:

- WhatsApp messages (end-to-end encryption)
- 🔐 Online banking and payment gateways
- 📧 Secure email communication
- 👥 Digital signatures & certificates

🎯 **Conclusion:**
Cryptography is like a **digital bodyguard** for your data 👮💻 — it makes sure only the right person can read or modify your information.

✔️ Q3 (12): What is MIME in Cryptography?

📦 What is MIME?

MIME stands for:

> **M**ultipurpose
> **I**nternet
> **M**ail
> **E**xtensions

📧 It is a standard that **extends the format of email messages** to support:

- 🖼️ Images
- 📎 Attachments
- 🎧 Audio & video
- 💻 Files like PDF, DOCX, etc.

🔐 What is MIME in Cryptography?

In **Cryptography**, MIME plays a key role in **securing email communication**.
It allows:

- Encryption of email content
- Digital signing of messages
- Sending **secure attachments** over email

👩 MIME is the **base** for advanced secure email technologies like **S/MIME (Secure MIME)**.

🔍 How MIME Helps in Secure Communication:

📌 Feature	🔐 Explanation
🛡️ Encryption Support	MIME allows email contents to be **encrypted**, making them unreadable to others
✍️ Digital Signatures	It supports **signing** emails to verify sender identity
🧩 File Encoding	Converts binary files into a **text format** for safe transmission
📎 Multiple Attachments	Helps attach and send **various file types securely** over one email

---

💡 Real-Life Example:

Imagine you're sending a project document to your teacher with a recorded explanation 🎤 and an image 📸:

➡️ Without MIME: Email can't handle those file types
With MIME: All files get attached, converted, and sent **securely and correctly** 📨🔐

🔑 What is S/MIME (Secure MIME)?

S/MIME is a protocol built on MIME that uses **cryptography** to:

- Encrypt emails
- ✍️ Digitally sign them
  It uses **public key encryption** to ensure that:
- Only the **intended recipient** can read the email
- The **sender is verified**

📜 Summary of MIME in Cryptography:

🔍 Point	💬 Details
📛 Full Form	Multipurpose Internet Mail Extensions
🎯 Purpose	To send **non-text files** & secure data via email
Use in Cryptography	Enables **encryption, authentication**, and file support
🌐 Extended As	S/MIME (Secure MIME) for high-level email security
✉️ Example Usage	Sending encrypted PDF report with your voice note

✔️ Conclusion:

MIME is like the **superpower of emails** 💌 — it turns a boring text email into a **secure digital package** 📦 with attachments, encryption, and authentication!

✔️ Q3 (13): Discuss about MIME in Detail

📦 MIME = Multipurpose Internet Mail Extensions

➡️ MIME is a **standard** used to **send emails with multiple types of content** like:

- 📄 Documents (PDF, Word)
- 🎧 Audio & 🎥 Video files
- 📷 Images
- 🧩 Applications or attachments

💬 Why Do We Need MIME?

Originally, email could **only send plain text** messages. But now we need to send:

- Resume
- Profile picture 📸
- Recorded introduction 🎤
  That's where **MIME** helps!

MIME **encodes these files** into a format email systems can handle 📧

🔐 MIME in Cryptography: Securing Email

MIME is the base for **S/MIME (Secure MIME)** which adds **cryptographic functions** like:

🔐 Security Function	💬 What It Does
🔒 Encryption	Hides the email content from others
✍️ Digital Signature	Verifies sender's identity
🧩 Encoding	Converts binary files to text for safe transfer

🧠 Example:

You're emailing your teacher your project report with your recorded explanation 🎤:

- MIME encodes the files
- S/MIME encrypts the email
- Ensures only the teacher can read it 🔐✔️

🧧 MIME Key Components:

🛠️ Component	🔎 Purpose
Content-Type	Tells what type of data (text, image, audio, etc.)
Content-Transfer-Encoding	Converts binary to ASCII format for safe email transport
Multipart	Allows attaching multiple files in a single email

✔️ Conclusion:

MIME turns your email into a **powerful, secure communication tool** 💌🛡️
It helps share **rich media** and **protects data privacy** through encryption & digital signatures.

✔️ Q3 (14): Discuss Cryptanalysis Techniques and Attacks in Detail

🧠 What is Cryptanalysis?

> Cryptanalysis is the science of **breaking cryptographic codes** without knowing the key 🔓💻

It's like being a digital detective 🕵️ trying to:

- **Decode messages**
- **Break encryption**
- **Find weaknesses in algorithms**

🎯 Goal of Cryptanalysis:

- Read hidden data 📜
- Change a message without being caught 🔄
- Prove that a system is **not secure**

🛠️ Techniques of Cryptanalysis:

🔍 Technique	💬 Explanation

🔍 Technique	💬 Explanation
1️⃣ **Brute Force Attack**	Try **every possible key** until the correct one is found 🗝️
2️⃣ **Frequency Analysis**	Analyze **letter frequencies** in cipher text to guess plain text 📊
3️⃣ **Known-Plaintext Attack**	Attacker has some plain text and cipher text pairs to guess the key 🔑
4️⃣ **Chosen-Plaintext Attack**	Attacker **chooses a plain text** and observes the cipher text result 🎯
5️⃣ **Chosen-Ciphertext Attack**	Attacker chooses cipher text and tries to get back the plain text 🔁
6️⃣ **Man-in-the-Middle Attack**	Attacker intercepts data between sender and receiver without their knowledge 👥

💣 Common Cryptanalysis Attacks:

🛡️ Attack Type	🧠 How It Works
🔓 **Ciphertext-only Attack**	Only cipher text is available. Try to guess the original message.
Known-Plaintext Attack	Uses known plain-cipher pairs to crack the encryption method.
Chosen-Plaintext Attack	Injects known plain text into the system to see how it's encrypted.
🔁 **Replay Attack**	Resends valid data to trick the system.
👥 **Man-in-the-Middle**	Intercepts and possibly changes messages between two parties.

💡 Real-Life Example:

> If a hacker sees multiple encrypted messages and guesses the algorithm, they might use **frequency analysis** to figure out common letters like **E, A, T, O** in English 🔤

✔️ Conclusion:

Cryptanalysis is like the **art of code-breaking** 🎨🔐
Understanding these attacks helps cybersecurity experts design **stronger encryption systems** to **protect our data** 🛡️💬

✔️ Q3 (15): What is Computer Security Attacks?

💻🔐 What is a Computer Security Attack?

> A **Computer Security Attack** is an action that attempts to **steal, damage, misuse, or disrupt** computer systems, data, or networks.

🦠 It is like a **digital crime** where hackers or malicious programs try to:

- 🕵️ Steal your data
- 💣 Destroy or modify files
- 🚫 Block access to your system

🚨 Types of Computer Security Attacks:

There are **4 major types of attacks** based on what they do to your system. Let's break them down one by one 👇

1️⃣ Interruption Attack 🚫

📌 Meaning:

This attack **disrupts or stops system services** so that users can't access them.

🔧 What it affects:

- System resources (like files, servers, devices)
- Network communication

🧠 Real-Life Example:

A **DDoS (Distributed Denial of Service)** attack floods a website with traffic, making it crash and go offline. Users can't access it anymore 🚫🌐

🛠️ Outcome:

- Service Unavailable ❌

- Data Loss 🗃️
- Downtime for businesses 🕒

2️⃣ Interception Attack 🕵️

📌 Meaning:

This attack **snoops or listens** to data that is **meant to be private**.

🔧 What it affects:

- Confidential messages 📧
- Data transfer over networks 🌐

🧠 Real-Life Example:

A hacker **sniffs unencrypted Wi-Fi** and reads your emails or passwords 📡🔓

🛠️ Outcome:

- Data Privacy Lost 🔐
- Sensitive Info Leaked 📝
- Identity Theft 👤

3️⃣ Modification Attack ✍️

Meaning:

This attack **alters the original data** or messages without permission.

What it affects:

- Stored data 🗂️
- In-transit messages 📩

Real-Life Example:

A hacker **changes your bank account number** in an online transaction, so money goes to them instead! 💸😱

🛠️ Outcome:

- Misinformation 📉
- Data Corruption 💾

- Financial Loss 💰

4️⃣ Fabrication Attack 🧪

📌 Meaning:

This attack **inserts fake data** or messages into a system.

🔧 What it affects:

- Logs 📜
- Emails 📩
- Authentication systems 🔐

🧠 Real-Life Example:

A fake user account is **created by a hacker** to gain unauthorized access into a system 🧑💻🚪

🛠️ Outcome:

- System Misuse
- False Information Generated 😵
- Fake Transactions or Access 🏦

📊 Summary Table:

🔢 Type	🔍 What It Does	🎯 Example
1️⃣ Interruption	Stops or damages service	Website crash via DDoS attack
2️⃣ Interception	Spies or listens to private communication	Hacker reading unencrypted emails
3️⃣ Modification	Changes original data	Altering payment details in an online transfer
4️⃣ Fabrication	Inserts fake data or messages	Creating fake accounts or login attempts

---

✔️ Conclusion:

Computer security attacks are like **invisible threats** 👻 that can **spy, block, change, or fake** data in your system.

Knowing these 4 types — **Interruption, Interception, Modification, and Fabrication** — helps us build **stronger, smarter protection** 🛡️👨‍💻
