Lecture – 06

A Trojan (short for Trojan Horse) is a type of malware that tricks users by pretending to be safe or useful software.

🔍 How Does It Work?

1. A Trojan looks like a real or helpful program.
2. But when you install or run it, it secretly does harmful actions in the background.
3. It does not spread by itself like viruses or worms. The user has to install it.

🛠 What Can a Trojan Do?

Once installed, a Trojan can:

1. Change or delete data
2. Steal your files
3. Export (send out) your private information
4. Destroy important system files
5. Install more malware secretly
6. Give control of your PC to hackers

💡 Example:

You download a **free antivirus software** from an unknown website.
It looks real, but it's a **Trojan**.
When you install it, it starts stealing your personal data instead of protecting your computer.

🕵 What is Spyware?

Spyware is a type of malware that hides in your computer and secretly watches what you do. It runs in the background without you knowing.

🔍 What Does Spyware Do?

It records your activities like:

1. What websites you visit
2. What you type (including passwords)
3. What files you open
4. Then it sends that information to a hacker or attacker.

📄 What Kind of Data Does It Steal?

Spyware can collect sensitive (private) information, such as:

1. Login credentials (username and password)
2. Banking details
3. Credit card numbers
4. Emails or private chats

💡 Example:

1. You install a game or tool from an untrusted website.
2. A spyware comes with it and starts recording everything you do.
3. Later, the hacker gets your bank account login from what you typed.

🔐 What is Ransomware?

Ransomware is a type of malware that locks or encrypts your files and then demands money (ransom) to give you back access.

😨 What Happens During a Ransomware Attack?

The malware enters your system (through email, fake links, or downloads).

It locks your computer or encrypts your files (makes them unreadable).

A message appears saying:

"Your files are locked."

"Pay money (usually in Bitcoin) to unlock them."

Even if you pay, there is no guarantee you will get your files back.

💡 Example:

You receive an email saying, “Click to view invoice.”

You click it, and ransomware installs on your PC.

All your photos, documents, and projects get locked.

A message asks you to pay $500 in Bitcoin to unlock them.

🎹 What is a Keylogger?

A **Keylogger** (also called **Keystroke Logger**) is a **tool or malware** that **records everything you type** on your keyboard.

.

🔍 What Does a Keylogger Do?

- It **monitors and saves** every keystroke (letter, number, password, etc.).
- This information can then be **sent to someone else** (like a hacker).

😇 Legitimate Uses of Keyloggers

- Sometimes used **legally** by:
  - Companies to **track employees' activity** on office computers.
  - Parents to monitor children’s internet use.
- In these cases, users usually know they’re being monitored.

😈 Malicious Use of Keyloggers

- **Cybercriminals** use keyloggers to:
  - Steal **login credentials**
  - Get **banking information**
  - Perform **identity theft**
  - **Blackmail** users using stolen private data

💡 Example:

You download a free game from an unsafe website.
A keylogger installs silently.
As you type your **email and password**, it gets sent to a hacker who uses it to **steal your identity**.

Prevention of Phishing Attacks

1. Know what a phishing scam looks like.
2. Don’t click on an unsolicited link
3. Get anti-phishing add-ons
4. Don’t give your information to an unsecured site
5. Rotate passwords regularly
6. Don’t ignore those updates
7. Install firewalls
8. Don’t be tempted by the pop-ups

9. Don’t give out important information unless you must
10. Have a Data Security Platform to spot signs of an attack

🎣 Phishing Attacks (Easy Notes)

📌 What is Phishing?

Phishing is a **type of cyberattack** where attackers **pretend to be someone trusted** (like a bank, company, or government agency) and **trick people into giving personal information**.

📩 How Do Phishing Attacks Work?

- Attackers send **fraudulent messages** via:
  - **Email** (common phishing)
  - **Text/SMS** → called **Smishing**
  - **Phone calls** → called **Vishing**
- The messages **look official** and ask the victim to:
  - Click a **link** that leads to a **fake website**
  - Download **attachments** (may contain malware)
  - Enter **personal data** like passwords, bank details, OTP, etc.

🏢 Common Fake Senders

- Banks (e.g., “Your account is locked”)
- Tax Offices
- Microsoft, Netflix, Telcos, ISPs
- Police or National Intelligence
- Online shops and delivery services

⚠️ Results of Phishing

- Theft of sensitive data
- Malware infection
- Identity theft
- Financial fraud

🎯 Types of Phishing Attacks

1. General Phishing

- Sent to a **large number of people**
- Looks generic (e.g., “Click here to win a prize!”)

---

2. Spear Phishing

- **Targets a specific person**
- Attacker gathers info from:
  - Social media
  - Online footprints
  - Dark Web
- Then sends a **personalized email** that looks trustworthy

---

3. Whaling

- Targets **high-profile people** like:
  - CEO
  - Managing Directors
  - Executives
- Aim: to steal credentials and access company data

---

4. Angler Phishing

- Happens on **social media**
- Scammer pretends to be a **customer service representative**
  - Example: A fake account like `@AmazonSupportHelp`
  - Replies to your post and sends you a link
  - Link leads to a phishing site to steal your info

✅ Rule of Thumb (to Stay Safe from Phishing)

📩 Always Be Careful with Unsolicited Messages

- If you get a message (email, SMS, or call) that you **didn’t expect**, especially from:
  - **Large organizations** (banks, Microsoft, Netflix, etc.)
  - **Government agencies**

    - **Telecom companies (Telcos)**

👉 **Do NOT trust it right away.** It could be a **phishing attempt**.

📞 Verify Before You Act

- **Do NOT click** on links or download attachments immediately.
- First, **verify the message** by:
    - Going to the **official website**
    - **Calling or emailing** the organization using **contact info from a trusted source**

⚠️ **Never reply** to the suspicious message or use the

contact info given in it — that might be fake too.

🧠 **Example:**

You get an email: "Your bank account is blocked. Click here to fix it."

Wrong Way: Clicking the link and entering your password
Right Way: Going to the bank's real website or calling customer service directly using their official phone number

---

Copyright, Designs, and Patents

Intellectual Property Rights (IPR) are legal rights that protect creative and innovative works.

Three key types of IPR:

• Copyright– Protects creative expressions.

• Designs– Protects the aesthetic appearance of products.

• Patents– Protect new inventions and technologies.

Comparison: Patent vs Design vs Copyright

Aspect	Patent	Design	Copyright
Definition	A legal right protects inventions and how they work.	Legal protection for a product's visual appearance.	Legal protection for original creative and intellectual works.
What It Protects	Functionality, structure, and operation of inventions.	Aesthetic aspects – shape, pattern, texture, and color of products.	Expression of ideas in literary, artistic, musical, and digital formats.
Scope of Protection	New inventions (e.g., machines, drugs, tech systems).	Product shapes, decorative patterns, packaging, and logos.	Books, music, art, films, software, websites, databases.
Example	A cancer drug was patented to stop unauthorized manufacturing.	Apple is registering the iPhone design to prevent visual imitation.	A musician copyrighting an album to stop illegal copies or remixes.
Duration	Typically, 20 years from the filing date.	Generally, 10–25 years, depending on jurisdiction.	Lifetime of the creator + 50 to 70 years (varies by country).
Focus	*How* something works.	*What* something looks like.	*How* something is expressed.
Significance	Promotes innovation, secures R&D investment, and prevents tech duplication.	Builds brand identity, boosts product appeal, and avoids design theft.	Encourages creativity, ensures financial rewards, and guards against plagiarism.
Legal Monopoly	Yes – gives exclusive production and usage rights.	Yes – prevents visual design imitation.	Yes – controls reproduction, distribution, and modification.
Permission Needed	Yes – to use, produce, or sell the patented invention.	Yes – to copy or reuse the registered design.	Yes – to reproduce, distribute, or alter the work.
Registration	Mandatory for protection.	Mandatory for enforcement in most cases.	Automatic upon creation (registration recommended for stronger enforcement).

Lecture 5

Given the scenario:
Sifat wants to send confidential information to **Urmi**, but:

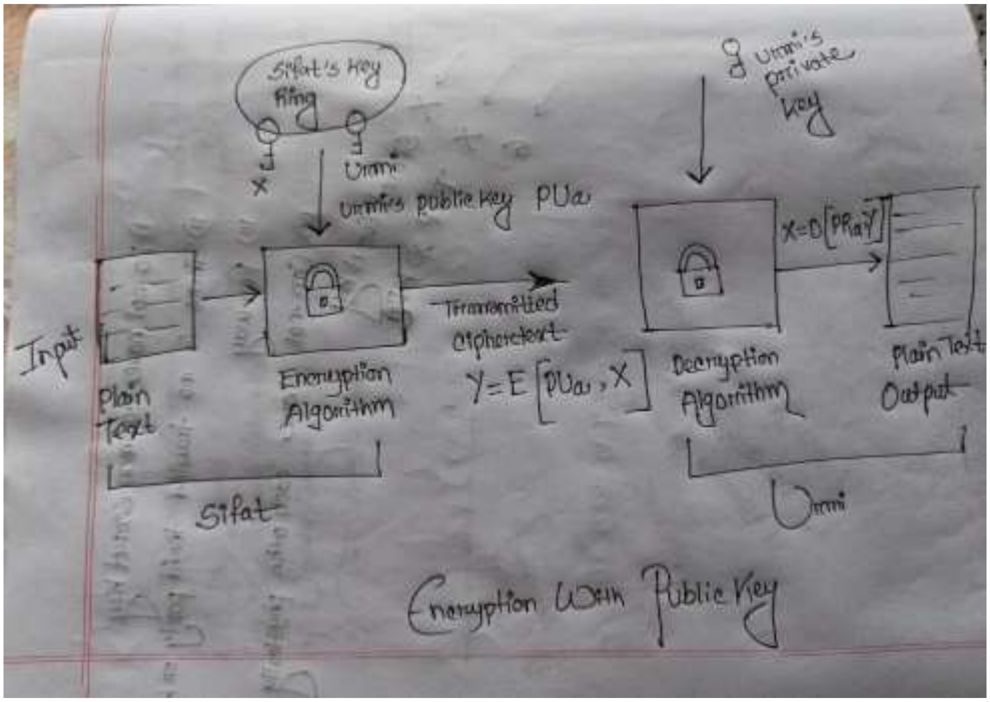
- They **don't have a shared secret key**
- There's **no trusted third party (TTP)** or **key distribution center (KDC)**
- And they are **far apart**, so they **can't exchange a key physically**

☑ Solution: **Public Key Cryptography (Asymmetric Encryption)**

Using public-key cryptography (as outlined in your lecture), Sifat and Urmi can securely communicate **without pre-sharing a secret key or relying on a third party.**

Six Ingredients of Public Key Cryptography:

1. Plaintext
2. Encryption Algorithm
3. Public
4. and Private Keys
5. Ciphertext
6. Decryption Algorithm



🔄 Step-by-Step Process

🔧 Step 1: Key Generation (By Urmi)

- Urmi generates a **key pair**:
  - Public Key: `PU_Urmi`
  - Private Key: `PR_Urmi`
- Urmi shares her **public key** `PU_Urmi` with Sifat (over email, website, or any open channel).

📤 Step 2: Sifat Encrypts the Message

- Sifat takes the confidential message `M`.
- He encrypts it using Urmi's **public key**:
  `C = Encrypt(PU_Urmi, M)`
- He sends the ciphertext `C` to Urmi.

📥 Step 3: Urmi Decrypts the Message

- Urmi receives ciphertext `C`.
- She decrypts it using her **private key**:
  `M = Decrypt(PR_Urmi, C)`

Now, only Urmi can decrypt the message, as **only she has the private key** `PR_Urmi`.

🔒 Symmetric vs Asymmetric Encryption

Feature	🔐 Symmetric Encryption	🔑 Asymmetric Encryption
Key Used	Single key (same for encryption & decryption)	Two keys (public key & private key)
Speed	Faster (lightweight operations)	Slower (computationally heavy)
Security Level	High, if the key is kept secret	Higher for open environments due to separate keys
Key Sharing	Requires a secure channel to share the key	No need for a secure channel; the public key is shared
Scalability	Difficult in large networks (many key pairs needed)	Scales well (just publish public keys)
Encryption/Decryption Cost	Low	High
Common Algorithms	AES, DES, Blowfish, RC4	RSA, ECC, ElGamal, DSA
Used For	Bulk data encryption, secure channels	Secure key exchange, digital signatures, and identity
Confidentiality	Achieved using a shared key	Achieved using the receiver’s public key
Authentication	Not directly supported	Supported (via digital signatures)
Key Management	Complex in multi-user systems	Easier public-key distribution