1. Cybersecurity and Its Importance

Definition:
Cybersecurity refers to the practices, technologies, and processes designed to protect systems, networks, and data from digital attacks, theft, or damage.

Importance of Cybersecurity:

- **Prevents Unauthorized Access:** Safeguards against unauthorized users trying to access sensitive data or systems.
- **Protects Against Financial Losses:** Prevents costly breaches, data theft, and ransomware attacks that result in financial damages.
- **Maintains Trust and Reputation:** Ensures the confidentiality and integrity of data, building trust with users, customers, and partners.
- **Compliance with Legal Requirements:** Ensures adherence to data protection laws and industry regulations, avoiding legal penalties.

2. Five Real-World Cyberattacks and How They Happened

1. **WannaCry Ransomware (2017)**
    - **Attack Method:** Exploited a vulnerability in outdated Windows systems (EternalBlue).
    - **Impact:** The ransomware spread rapidly, encrypting files and demanding ransom payments in Bitcoin.
    - **Outcome:** Global impact, affecting organizations like the NHS in the UK.
2. **Yahoo Data Breach (2013-2014)**
    - **Attack Method:** Hackers accessed both encrypted and plaintext security questions and answers.
    - **Impact:** Affected 3 billion accounts due to weak security practices.
    - **Outcome:** One of the largest data breaches in history, damaging Yahoo's reputation.
3. **SolarWinds Supply Chain Attack (2020)**
    - **Attack Method:** Hackers inserted malicious code into software updates from SolarWinds, a popular IT management company.
    - **Impact:** Allowed attackers to infiltrate several high-profile government and corporate networks.
    - **Outcome:** Widespread breach with significant geopolitical consequences.

4. **Target Data Breach (2013)**

    - **Attack Method:** Hackers accessed third-party vendor credentials to infiltrate Target's systems.
    - **Impact:** Credit card information of over 40 million customers was stolen.
    - **Outcome:** Financial losses and reputational damage for Target.
5. **Colonial Pipeline Ransomware Attack (2021)**

    - **Attack Method:** DarkSide ransomware targeted the IT systems of Colonial Pipeline, disrupting fuel supply operations.
    - **Impact:** Attackers demanded a $4.4 million ransom, causing widespread fuel shortages in the U.S.
    - **Outcome:** The attack raised concerns over critical infrastructure vulnerability.

3. Difference Between HTTP and HTTPS

HTTP (HyperText Transfer Protocol):

- **Definition:** A protocol used for transferring data between a web server and a browser in plaintext.
- **Vulnerabilities:** Data sent over HTTP can be intercepted by attackers, exposing sensitive information like login credentials and payment details.

HTTPS (HyperText Transfer Protocol Secure):

- **Definition:** A secure version of HTTP, using SSL/TLS encryption to protect the data being transferred.
- **Benefits:**
    - **Encryption:** Protects sensitive data (e.g., passwords, credit card info) from interception.
    - **Data Integrity:** Ensures the data received is exactly what was sent, without tampering.
    - **Authentication:** Verifies the identity of the website, reducing the risk of man-in-the-middle attacks.

4. AES and RSA Encryption

1. AES (Advanced Encryption Standard)

- **Type:** Symmetric encryption (same key for both encryption and decryption).
- **Example:**
    - **Encryption:** Message "Hello" is encrypted using key "1234".
    - **Decryption:** Using the same key "1234", the encrypted text is converted back to "Hello".
- **Use Case:** Efficient for encrypting large volumes of data, such as files or entire disks.

2. RSA (Rivest–Shamir–Adleman)

- **Type:** Asymmetric encryption (uses a public key for encryption and a private key for decryption).
- **Example:**
    - **Encryption:** A message "Secret" is encrypted using a public key.
    - **Decryption:** The encrypted message is decrypted using the corresponding private key.
- **Use Case:** Ideal for secure communication over open networks and for digital signatures.