**1. What is Cyber Security and why is it important?**

**Ans**. **Definition** - Cybersecurity safeguards digital systems, networks, and data from unauthorized access, theft, or damage, ensuring information confidentiality, integrity, and availability.

**Importance** – **i)** Safeguards sensitive information, including personal data and financial transactions. **ii)** Prevents disruptions to businesses and individuals worldwide. **iii)** Essential in today’s interconnected world with rising cyber threats**. iv)** Vital for protecting assets and data against hackers. **v)** Ensures the survival and resilience of organizations.

**2. Five real-world cyberattacks and how they happened.**

**Ans. A) WannaCry Ransomware Attack (2017) -** Exploited a Windows vulnerability (EternalBlue), leaked from the NSA. Systems without updated patches were targeted.

**B) SolarWinds Supply Chain Attack (2020) -** Attackers infiltrated SolarWinds' development environment, embedding a backdoor in software updates.

**C) Equifax Data Breach (2017) -** Hackers exploited a known vulnerability in Apache Struts, which Equifax had failed to patch.

**D)** **Target Data Breach (2013) -** Gained access via a third-party HVAC vendor’s credentials and installed malware on Target’s POS systems.

**E)** **Colonial Pipeline Ransomware Attack (2021) -** Attackers used a compromised password to access the network via a VPN without multifactor authentication.

**3. Difference between HTTP and HTTPS**.

**Ans. HTTP HTTPS**

HyperText Transfer Protocol HyperText Transfer Protocol Secure

Unsecured (No data Encryption) Secured (data encryption using SSL/TLS)

Operates in port 80 operates on port 443

Suitable for non-sensitive websites Essential for e-commerce, banking etc.

No padlock icon showing not secure Padlock icon showing security.

URL- http//: URL – https//:

**4. Explanation of AES and RSA encryption with simple examples.**

**Ans. \*\*AES (Advanced Encryption Standard)** is a symmetric encryption method, meaning the same key is used for both encryption and decryption. A secret key encrypts the data into ciphertext. The same key is required to decrypt the ciphertext back to the original data.

**Example** - **Plaintext**: "My name is Harshita Dubey"

**Key**: "2507"

**Encryption**: The plaintext is converted to ciphertext.

**Decryption**: Using the same key ("2507"), the ciphertext is converted back to "My name is Harshita Dubey".

**\*\*RSA (Rivest-Shamir-Adleman)** is an asymmetric encryption method using two keys: **Public Key**: Used to encrypt data. **Private Key**: Used to decrypt data.

**Example - Public Key**: (shared publicly), **Private Key**: (kept secret by the recipient), **Plaintext**: "Harshita"

The sender encrypts "Harshita" using the recipient’s public key, resulting in ciphertext.

The recipient decrypts it with their private key to retrieve "Harshita".