1.What is cyber security and why is it important?

Cyber security: Cybersecurity means protecting your systems, networks, and data from online attacks, unauthorized access, or theft. It uses tools and strategies to keep your information safe, private, and accessible only to the right people. Cybersecurity acts like a digital shield, keeping you and your information safe from hackers, viruses, and other online dangers.

Why is it important

Cybersecurity is important because it keeps our personal information, money and online activities safe from hackers like passwords and bank account details.

1. Protects Sensitive Data
2. Maintains national security
3.Prevents Online Fraud and Scams
4. Ensures Business Continuity

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

1. **State bank of India (2017-Data Breach):** Sensitive customer data including personal details and bank account information, were reportedly leaked online due to vulnerabilities in SBI's System.
2. **Indian Air Force (2019 – Phishing Attack):** A phishing attack targeted the Indian Air Force, where emails containing malware were sent to military personnel to steal sensitive data and intelligence.
3. **Indian Government Websites (2020- DDoS Attack):** Several Indian Government websites face Distributed Denial of service attacks.
4. **Aadhaar Data Breach (2018):** Hackers reportedly gained access to Aadhaar data, including sensitive personal information of over 1 billion citizens.
5. **Jammu and Kashmir Cyber Attack (2019):** Hackers used spear-phishing to steal confidential security and government data.

3.Difference between HTTP and HTTPS.

HTTP	HTTPS
No encryption - Data is sent unprotected.	Encrypted – Ensures data privacy and security.
Port 80 – Standard port for combination.	Port 443 – Standard port for secure communication.
No server authentication – No identity verification.	Server authentication – Verifies website identity with SSL certificate
Used for non-sensitive sites – E.g. informational websites.	Used for sensitive sites – E.g. online banking, shopping.
Faster – No encryption overhead.	Slightly slower - Due to encryption process.

4.AES and RSA:

AES (Advanced Encryption Standard): A symmetric encryption method where the same key is used for both encryption and decryption. Example: Encrypting a file with a password.

RSA (Rivest-Shamir-Adleman): An asymmetric encryption method using a public key for encryption and a private key for decryption. Example: Secure email where only the recipient can decrypt the message.