Task 1: Research & Documentation:

Ques. 1: What is cybersecurity, and why is it important?

Ans : Cybersecurity involves the practices, technologies, and processes designed to protect computers, networks, devices, and data from attacks, damage, or unauthorized access. It encompasses a wide range of measures to safeguard sensitive information from cyber threats, including malware, phishing, ransomware, hacking, and other forms of cybercrime.

Why is it important?

- Protects Sensitive Data: Cybersecurity helps safeguard personal, financial, and business information from being stolen or compromised.
- Prevents Financial Loss: Cyberattacks can lead to significant financial losses for individuals and organizations. Strong cybersecurity measures help prevent such losses.
- Maintains Privacy: It ensures that personal and confidential information remains private and is not accessed or misused by unauthorized individuals.
- Ensures Business Continuity: Businesses rely on cybersecurity to protect their operations and ensure that their services and activities continue without disruption.
- Builds Trust: Effective cybersecurity measures build trust among customers, clients, and stakeholders, knowing that their data is secure.
- Protects Critical Infrastructure: It is vital for safeguarding essential services such as power grids, transportation systems, and healthcare facilities from cyber threats.

Ques. 2: Five real-world cyberattacks and how they happened.

Ans : The five real-world cyberattacks are :

1. Aadhaar Data Breach (2018):
    - How it happened: Unauthorized access to Aadhaar, India's national identification system, exposed the personal data of over 1.1 billion citizens. The breach was facilitated by the lack of robust security measures and proper encryption.
    - Impact: The breach raised concerns about data privacy and the security of sensitive personal information, prompting calls for stronger data protection regulations.
2. Cosmos Bank Cyberattack (2018):
    - How it happened: Hackers infiltrated Cosmos Bank's ATM server and cloned debit cards to withdraw approximately ₹94.42 crores ($13.5 million) from ATMs across 28 countries over two days. The attack involved malware and coordinated withdrawals by cybercriminals.

- Impact: The bank faced significant financial losses and reputational damage, highlighting vulnerabilities in banking systems and the need for enhanced cybersecurity measures.

3. BSNL Data Breach (2017):
    - How it happened: An unsecured database of Bharat Sanchar Nigam Limited (BSNL) exposed the personal information of around 47,000 employees. The breach occurred due to a misconfiguration in the database, allowing unauthorized access.
    - Impact: The breach exposed sensitive employee information, leading to concerns about data security practices within government-owned organizations.
4. Wannacry Ransomware Attack (2017):
    - How it happened: The global WannaCry ransomware attack also impacted various organizations in India, including government offices, private companies, and healthcare institutions. The ransomware encrypted files and demanded ransom payments in Bitcoin.
    - Impact: The attack disrupted operations and caused financial losses, emphasizing the need for regular software updates and robust cybersecurity practices.
5. Union Bank of India Cyberattack (2016):
    - How it happened: Hackers used a phishing email to gain access to Union Bank of India's SWIFT (Society for Worldwide Interbank Financial Telecommunication) system. They attempted to transfer $171 million to offshore accounts but were thwarted by timely intervention.
    - Impact: The bank managed to recover most of the funds, but the incident underscored the importance of employee training and awareness in preventing phishing attacks.

Ques. 3: Difference between HTTP and HTTPS.

Ans : Key Differences:

- Encryption:
    - HTTP: No encryption; data is sent in plain text.
    - HTTPS: Uses SSL/TLS encryption to secure data.
- Security:
    - HTTP: Vulnerable to interception and attacks.
    - HTTPS: Provides a secure and encrypted connection, protecting data integrity and confidentiality.

- Trustworthiness:
    - HTTP: Less secure, may not be trusted for sensitive transactions.
    - HTTPS: Trusted for secure transactions like online banking, shopping, and login information.

Ques. 4: Explanation of AES and RSA encryption with simple examples.

Ans : AES (Advanced Encryption Standard) : AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. It is widely used due to its efficiency and strong security.

Example:

- Step 1: Plaintext: Let's say you have the message "Hii".
- Step 2: Encryption Key: You and the recipient share a secret key, e.g., "123".
- Step 3: Encryption: Using AES, the message "Hii" is encrypted with the key "123" to produce a ciphertext (let's pretend it's "X89$#").
- Step 4: Decryption: The recipient uses the same key "123" to decrypt "X89$#" back into "Hii".

In this example, both parties must keep the key secret to maintain security. If anyone else gets the key, they can decrypt the messages.

RSA (Rivest-Shamir-Adleman) : RSA is an asymmetric encryption algorithm, meaning it uses a pair of keys: a public key for encryption and a private key for decryption. The public key is shared with everyone, while the private key is kept secret.

Example:

- Step 1: Key Generation: You generate a pair of keys: a public key (e.g., "PublicKey123") and a private key (e.g., "PrivateKey789").
- Step 2: Plaintext: Let's say someone wants to send you the message "HELLO".
- Step 3: Encryption: They use your public key "PublicKey123" to encrypt "HELLO" into a ciphertext (let's pretend it's "QWERTY").
- Step 4: Decryption: You use your private key "PrivateKey789" to decrypt "QWERTY" back into "HELLO".

In this example, even if someone intercepts the ciphertext "QWERTY", they cannot decrypt it without your private key.