R. C. PATEL
INSTITUTE OF TECHNOLOGY
An Autonomous Institute

Shri. Amrishbhai Patel
President
Prof. Dr. J. B. Patil
Director

Near Nimzari Naka, Shahada Road,
Shirpur-425405, Dist: Dhule (MS)
Telefax: (02563) 259600,801,802
Web: www.rcpit.ac.in
www.facebook.com/shirpurrcpit
Email: director@rcpit.ac.in

Department of Computer Engineering

(Shortlisted Mock Interview Questions)

Course: Information Security (22PCCO6030T) **Class:** T.Y. B. Tech.

Name of Faculty: Mr. Vishal S. Thakare, Ms J. S. Sonawane

Q. No.	Interview Question	Answer
1	**What is Cryptography?**	• Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for. • It is a technique through which we convert a plain text to cipher text and cipher text to plain text. • Plain text is a message that can be understood and read by any human, whereas Cipher text is an encrypted message that can only be read but cannot be understood. • Plain text is converted to cipher text using a key and vice versa. With this key, we can decode the cipher text into plain text.
2	**What is the difference between IDS and IPS?**	• **IDS** is **Intrusion Detection System** and it only detects intrusions and the administrator has to take care of preventing the intrusion. • **IPS** i.e., **Intrusion Prevention System**, the system detects the intrusion and also takes actions to prevent the intrusion.
3	**How is Encryption different from Hashing?**	• Both Encryption and Hashing are used to convert readable data into an unreadable format. • The difference is that the encrypted data can be converted back to original data by the process of decryption but the hashed data cannot be converted back to original data.
4	**What is a Firewall and why is it used?**	• A Firewall is a network security system set on the boundaries of the system/network. • It monitors and controls the incoming and outgoing network traffic based on an organization's previously established security policies. • Firewalls are mainly used to protect the system/network from viruses, worms, malware, etc. Firewalls can also be to prevent remote access and content filtering.

5	**What is phishing?**	• Phishing is a type of cyber-attack. • It involves sending fake emails and messages to trick people into providing sensitive information, including credit card details and passwords. • It can be carried out through social media, phone calls, or SMS messages.
6	**What does XSS stand for? How can it be prevented?**	• XSS is an abbreviation for cross-site scripting. • Cross-site scripting (XSS) is a vulnerability in web applications that allows third parties to execute scripts on behalf of the web application in the user's browser. **To prevent XSS:** • **Validate and sanitize user input** • **Escape output before rendering in HTML** • **Use secure frameworks** like React/Angular • **Implement Content Security Policy (CSP)**
7	**What do you mean by Network Sniffing?**	• Network Sniffing is a passive approach for monitoring network communication, decoding protocols, and inspecting headers and payloads for relevant information. • It is a technique for both identifying and analysing targets. • Sniffers are used by attackers to capture data packets including sensitive passwords and account information.
8	**What is cyber security?** **(Clover Infotech)**	• Cyber security is the practice of protecting systems, networks, and programs from digital attacks. • It involves using a variety of security measures to prevent unauthorized access, data breaches, and other cyber threats.
9	**What is a Denial of Service attack?**	• A Denial of Service attack is a cyber-attack that aims to disturb the functioning of a network or website. • It does so by sending a massive volume of traffic to the target website from multiple sources; this makes it impossible to respond to any user requests or messages on the website. • This results in financial and reputational damage.
10	**What is the man-in-the-middle attack?**	• This is a type of cyber-attack in which the attacker stays between the two to carry out their mission. • The type of function it can perform is to modify the communication between two parties so that both parties feel like they are communicating over a secure network.