NETWORK SECURITY
QUESTION BANK

PART A – 2 Mark Questions with Answers | PART B – 16 Mark Questions

UNIT I – FUNDAMENTALS OF NETWORKING SECURITY

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is Network Security?	Network security refers to the policies, practices, and technologies used to protect computer networks and data from unauthorized access, misuse, or attacks.
2	What is Confidentiality in security?	Confidentiality ensures that information is accessible only to authorized users and is not disclosed to unauthorized parties. Example: encryption.
3	What is Authentication?	Authentication is the process of verifying the identity of a user or system to ensure that they are who they claim to be.
4	What is Data Integrity?	Data integrity ensures that information has not been altered or tampered with during transmission. It is verified using hashing algorithms like SHA.
5	What is Non-repudiation?	Non-repudiation ensures that a party cannot deny having sent or received a message. It is achieved using digital signatures.
6	What is Access Control?	Access control restricts access to resources based on identity and authorization, ensuring only permitted users can access specific data or systems.
7	What is Availability in security?	Availability ensures that authorized users have reliable and timely access to information and resources whenever needed.
8	What is an Interruption attack?	An interruption attack is a security attack where the availability of a resource is disrupted, such as a Denial-of-Service (DoS) attack.
9	What is an Interception attack?	An interception attack is when an unauthorized party gains access to data during transmission. Example: eavesdropping, packet sniffing.
10	What is a Modification attack?	A modification attack occurs when an attacker intercepts and alters data in transit before forwarding it to the recipient.

11	What is a Fabrication attack?	A fabrication attack involves creating counterfeit data or messages and inserting them into a system to deceive recipients.
12	Differentiate active and passive attacks.	Passive attacks (interception) only monitor data without altering it. Active attacks (modification, fabrication) alter or disrupt data and systems.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain the overview of Network Security. Discuss the various Security Services: Confidentiality, Authentication, Integrity, Non-repudiation, Access Control, and Availability with examples.
2	Describe the Security Mechanisms used to implement security services. Explain each mechanism with suitable examples.
3	Explain the four types of Security Attacks: Interruption, Interception, Modification, and Fabrication with diagrams and examples.
4	Discuss the relationship between Security Services, Mechanisms, and Attacks (X.800 model). How do services counter specific attacks?
5	Explain the CIA Triad (Confidentiality, Integrity, Availability) in detail. Why is each component critical in network security?

UNIT II – AUTHENTICATION AND SECURITY

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is Authentication?	Authentication is the process of verifying the identity of a user or entity claiming to be someone, using passwords, tokens, or biometrics.
2	What is a Key Exchange Protocol?	A key exchange protocol is a method by which two parties establish a shared cryptographic key over an insecure channel. Example: Diffie-Hellman.
3	What is the Diffie-Hellman key exchange?	Diffie-Hellman is a key exchange protocol that allows two parties to generate a shared secret key over an insecure channel without prior shared secrets.
4	What is Mediated Key Exchange?	In mediated key exchange, a trusted third party (Key Distribution Center/KDC) helps establish session keys between communicating parties. Example: Kerberos.
5	What is Password-Based Authentication?	Password-based authentication verifies identity by comparing user-provided passwords with stored credentials, often hashed for security.
6	What is Password Security?	Password security involves protecting passwords through hashing (e.g., bcrypt), salting, minimum length requirements, and multi-factor authentication.
7	What is a Certificate Authority (CA)?	A CA is a trusted entity that issues digital certificates, binding a public key to an individual or organization's identity.
8	What is a Digital Signature?	A digital signature is a cryptographic mechanism that provides authentication, non-repudiation, and integrity by signing data with a private key.
9	What is a Digital Certificate?	A digital certificate is an electronic document issued by a CA that contains a public key, owner identity, and CA signature to authenticate entities.
10	What is Key Management?	Key management involves the generation, distribution, storage, rotation, and revocation of cryptographic keys to maintain security.
11	What is the challenge-response protocol?	In challenge-response, a verifier sends a challenge (random number) and the claimant must respond correctly (using a shared secret or private key) to prove identity.
12	What is Kerberos?	Kerberos is a network authentication protocol using tickets and a trusted KDC (Key Distribution Center) for secure mutual authentication in a distributed system.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain Authentication protocols in detail. Discuss password-based authentication, challenge-response, and Kerberos with diagrams.
2	Explain Key Exchange protocols: Diffie-Hellman key exchange and mediated key exchange (KDC/Kerberos) with step-by-step examples.
3	Explain Digital Signatures: working principle, creation, verification, and the role of public-key cryptography. Give examples.
4	Explain Certificate Authority (CA) and key management: certificate issuance, certificate chain, certificate revocation, and PKI infrastructure.
5	Explain Digital Certificates and their role in authentication. Discuss the X.509 certificate format and its fields in detail.

UNIT III – PUBLIC-KEY CRYPTOGRAPHY AND MESSAGE AUTHENTICATION

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is Cryptography?	Cryptography is the science of securing information by transforming it into an unreadable format using algorithms and keys, readable only by authorized parties.
2	What is a Cryptographic Hash Function?	A cryptographic hash function maps input data of any size to a fixed-size digest. It is one-way, deterministic, and collision-resistant. Examples: MD5, SHA-256.
3	What is Symmetric Encryption?	Symmetric encryption uses the same key for both encryption and decryption. It is fast but requires secure key sharing. Examples: AES, DES.
4	What is Public-Key (Asymmetric) Encryption?	Public-key encryption uses a pair of keys (public for encryption, private for decryption). It solves key distribution problems. Example: RSA.
5	What is RSA?	RSA is a widely used public-key cryptography algorithm based on the difficulty of factoring large integers, used for encryption and digital signatures.
6	What is a Cipher Block Mode?	Cipher block modes define how block ciphers encrypt data larger than the block size. Modes include ECB, CBC, CFB, OFB, and CTR.
7	What is CBC mode?	CBC (Cipher Block Chaining) mode XORs each plaintext block with the previous ciphertext block before encryption, adding dependency between blocks.
8	What is SHA?	SHA (Secure Hash Algorithm) is a family of cryptographic hash functions (SHA-1, SHA-256, SHA-512) standardized by NIST for data integrity.
9	What is HMAC?	HMAC (Hash-based Message Authentication Code) combines a cryptographic hash function with a secret key to provide both data integrity and authentication.
10	What is the difference between a hash and encryption?	Hashing is a one-way function producing a fixed digest (not reversible). Encryption is two-way: data can be decrypted with the right key.
11	What are the principles of Public-Key Cryptography?	Public-key cryptography is based on mathematical one-way functions: easy to compute in one direction but computationally infeasible to reverse without the private key.
12	What is ECB mode?	ECB (Electronic Codebook) mode encrypts each block independently with the same key. It is simple but insecure as identical plaintext blocks produce identical ciphertext.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain the basics of Cryptography: types (symmetric, asymmetric), key concepts, and the differences between them with examples.
2	Explain Public-Key Cryptography principles and the RSA algorithm in detail with key generation, encryption, and decryption steps.
3	Describe Cipher Block Modes of Operation: ECB, CBC, CFB, OFB, and CTR modes with diagrams and their advantages/disadvantages.
4	Explain Secure Hash Functions (SHA family) in detail. Discuss properties of a secure hash function and the SHA-256 algorithm.
5	Explain HMAC (Hash-based Message Authentication Code): structure, working, security properties, and how it differs from simple hashing.

UNIT IV – SECURITY ATTACKS

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is a Buffer Overflow attack?	A buffer overflow attack occurs when a program writes more data to a buffer than it can hold, overwriting adjacent memory and allowing code execution.
2	What is a Format String Vulnerability?	A format string vulnerability arises when user input is passed directly as a format string to functions like printf(), allowing attackers to read/write memory.
3	What is a Denial-of-Service (DoS) attack?	A DoS attack floods a system, server, or network with traffic to exhaust resources, making it unavailable to legitimate users.
4	What is a DDoS attack?	A DDoS (Distributed Denial-of-Service) attack uses multiple compromised machines (botnet) simultaneously to overwhelm a target with traffic.
5	What is TCP Session Hijacking?	TCP session hijacking is an attack where an attacker takes over a legitimate TCP session by predicting sequence numbers and injecting malicious packets.
6	What is ARP Spoofing?	ARP spoofing sends fake ARP replies to associate the attacker's MAC address with a legitimate IP, intercepting network traffic.
7	What is a Man-in-the-Middle (MITM) attack?	In a MITM attack, the attacker secretly intercepts and possibly alters communications between two parties who believe they are communicating directly.
8	What is a Computer Virus?	A computer virus is malicious code that attaches itself to legitimate programs, replicates, and can damage files, systems, or steal data.
9	What is Spyware?	Spyware is malicious software that secretly monitors user activity, collects personal information, and sends it to a third party without user consent.
10	What is Phishing?	Phishing is a social engineering attack where attackers impersonate legitimate entities via email or websites to trick users into revealing sensitive information.
11	What is a Botnet?	A botnet is a network of compromised computers (bots) controlled by an attacker (botmaster) to perform coordinated attacks like DDoS or spam.
12	What is Route Table Modification?	Route table modification is an attack where an attacker alters routing tables to redirect network traffic through malicious nodes for interception.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain Buffer Overflow attacks and Format String vulnerabilities in detail: how they occur, examples, and defenses.
2	Explain Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks: types, how they work, tools used, and countermeasures.
3	Explain Hijacking attacks: TCP session hijacking, ARP attacks, UDP hijacking, and Man-in-the-Middle attacks with defenses.
4	Explain Internet worms, viruses, spyware, phishing, and botnets: how they spread, their impact, and prevention techniques.
5	Explain route table modification and UDP hijacking attacks. How do these attacks affect network communication and how can they be mitigated?

UNIT V – IP SECURITY AND WEB SECURITY

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is a Firewall?	A firewall is a network security device that monitors and controls incoming and outgoing traffic based on predefined security rules.
2	What is a VPN?	A VPN (Virtual Private Network) creates an encrypted tunnel over a public network to provide secure, private communication between endpoints.
3	What is an Intrusion Detection System (IDS)?	An IDS monitors network traffic or system activity for suspicious behavior and alerts administrators to potential threats.
4	What is PGP?	PGP (Pretty Good Privacy) is an email encryption standard that uses public-key cryptography to provide confidentiality, authentication, and integrity for emails.
5	What is S/MIME?	S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data (email), providing authentication and confidentiality.
6	What is SSL?	SSL (Secure Sockets Layer) is a cryptographic protocol that provides secure communication over a network by encrypting data between client and server.
7	What is TLS?	TLS (Transport Layer Security) is the successor to SSL, providing improved encryption, authentication, and integrity for network communications.
8	What is IPsec?	IPsec (Internet Protocol Security) is a suite of protocols that authenticate and encrypt IP packets, securing communications at the network layer.
9	What is IKE?	IKE (Internet Key Exchange) is the protocol used to set up a security association (SA) and negotiate keys for IPsec connections.
10	What is DNS Security (DNSSEC)?	DNSSEC adds cryptographic signatures to DNS records to protect against DNS spoofing and cache poisoning attacks.
11	What is SET?	SET (Secure Electronic Transaction) is a protocol developed by Visa and MasterCard for securing credit card transactions over the internet.
12	What is Wireshark?	Wireshark is an open-source network protocol analyzer (packet sniffer) used to capture and analyze network traffic for troubleshooting and security analysis.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain network defense tools: Firewalls (types: packet filter, stateful, application layer), VPNs, and Intrusion Detection Systems (IDS/IPS) with diagrams.
2	Explain Email Privacy: PGP (Pretty Good Privacy) and S/MIME. Discuss how each provides confidentiality, authentication, and integrity for emails.
3	Explain SSL and TLS protocols in detail: handshake process, key exchange, record protocol, and how they secure web communications.
4	Explain IPsec architecture and IKE: AH and ESP protocols, transport vs tunnel mode, and the Internet Key Exchange (IKE) negotiation process.
5	Explain DNS Security (DNSSEC) and Secure Electronic Transaction (SET). Discuss threats addressed and how each protocol provides security.