U23CBT43 - CRYPTOGRAPHY AND CYBER SECURITY

Question Bank: 2 Mark Q&A + 16 Mark Questions (Unit I to V)

UNIT I – INTRODUCTION TO SECURITY

PART A – 2 Mark Questions with Answers

1. Define Computer Security.

Computer Security is the protection of computer systems and information from unauthorized access, damage, theft, or disruption. It ensures Confidentiality, Integrity, and Availability (CIA triad) of data and resources.

2. What is the OSI Security Architecture?

The OSI Security Architecture (X.800) defines a framework for security services and mechanisms. It covers Security Attacks (passive/active), Security Services (confidentiality, authentication, etc.), and Security Mechanisms (encryption, digital signatures, etc.).

3. Differentiate Active and Passive Attacks.

Passive attacks monitor or eavesdrop on transmissions without modifying data (e.g., traffic analysis, eavesdropping). Active attacks modify or forge data (e.g., masquerade, replay, modification, denial of service). Passive attacks are hard to detect; active attacks are hard to prevent.

4. What are Security Services?

Security Services are services defined by X.800 to counter security attacks: (i) Confidentiality, (ii) Authentication, (iii) Integrity, (iv) Non-repudiation, (v) Access Control, and (vi) Availability.

5. What are Security Mechanisms?

Security Mechanisms are tools used to implement security services. Examples: Encipherment (encryption), Digital Signatures, Access Control, Data Integrity checks, Authentication Exchange, Traffic Padding, Routing Control, Notarization.

6. What is a Model for Network Security?

The Network Security Model shows how a message is securely transmitted: Sender encrypts the message using a security-related transformation and a secret key; the receiver decrypts it. A Trusted Third Party (e.g., key distributor) may assist.

7. What is a Classical Encryption Technique?

Classical encryption techniques are historical ciphers used before modern cryptography. They include Substitution ciphers (replace characters) and Transposition ciphers (rearrange characters). Examples: Caesar cipher, Vigenere cipher, Rail Fence cipher.

8. What is a Substitution Technique?

A Substitution Technique replaces each character or bit of plaintext with another character or bit. Examples: Caesar Cipher (shifts letters by fixed number), Monoalphabetic Cipher, Playfair Cipher, and Vigenere Cipher.

9. What is a Transposition Technique?

A Transposition Technique rearranges the characters in the plaintext without changing them. Examples: Rail Fence Cipher (writes in zigzag pattern), Row Transposition Cipher (writes row-wise, reads column-wise).

10. What is Steganography?

Steganography is the practice of hiding secret information within ordinary, non-secret data (like images, audio, or text) to avoid detection. Unlike encryption which hides content, steganography hides the existence of the message.

PART B – 16 Mark Questions

1. Explain the OSI Security Architecture (X.800) in detail. Describe Security Attacks, Security Services, and Security Mechanisms with examples.

2. Describe the Classical Encryption Techniques. Explain Caesar Cipher, Playfair Cipher, Hill Cipher, Vigenere Cipher, and Rail Fence Cipher with examples.

3. Explain the Model for Network Security. Describe how security services and mechanisms work together to protect communication over a network.

4. Differentiate between Active and Passive attacks. Explain types of each with examples and prevention strategies.

5. Explain Substitution and Transposition techniques in detail. Also explain Steganography and how it differs from cryptography.

UNIT II – SYMMETRIC CIPHERS

PART A – 2 Mark Questions with Answers

1. What is Symmetric Key Cryptography?

Symmetric Key Cryptography uses the same key for both encryption and decryption. Both sender and receiver must share the secret key securely. It is fast and efficient for large data. Examples: DES, AES, RC4.

2. What is SDES (Simplified DES)?

S-DES (Simplified DES) is a simplified version of DES designed for educational purposes. It operates on 8-bit plaintext using a 10-bit key, producing 8-bit ciphertext through two rounds of permutation, substitution, and key mixing.

3. What is DES (Data Encryption Standard)?

DES is a symmetric block cipher that encrypts 64-bit blocks using a 56-bit key through 16 rounds of Feistel structure. Each round uses permutation, substitution (S-boxes), and key mixing. Though now considered insecure, it laid the foundation for modern ciphers.

4. What is the Strength of DES?

DES uses a 56-bit key, giving 2^56 (about 72 quadrillion) possible keys. Its strength lies in confusion (S-boxes) and diffusion (permutations). However, it is vulnerable to brute-force attacks and differential/linear cryptanalysis.

5. What is Differential Cryptanalysis?

Differential Cryptanalysis is a chosen-plaintext attack that studies how differences in input pairs affect the output differences after encryption. It exploits the non-random behavior of S-boxes to recover the secret key with fewer operations than brute force.

6. What is Linear Cryptanalysis?

Linear Cryptanalysis is a known-plaintext attack that finds linear approximations between plaintext bits, ciphertext bits, and key bits. It uses these approximations to deduce key bits statistically from a large number of plaintext-ciphertext pairs.

7. What is AES (Advanced Encryption Standard)?

AES is a symmetric block cipher that replaced DES. It operates on 128-bit blocks with key sizes of 128, 192, or 256 bits through 10, 12, or 14 rounds respectively. Each round uses SubBytes, ShiftRows, MixColumns, and AddRoundKey operations.

8. What are Block Cipher Modes of Operation?

Block cipher modes define how to encrypt data longer than one block: ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), and CTR (Counter). CBC is most commonly used for its security properties.

9. What is RC4?

RC4 is a symmetric stream cipher designed by Ron Rivest. It generates a pseudorandom keystream that is XORed with plaintext to produce ciphertext. RC4 is simple and fast but has known vulnerabilities and is no longer recommended for secure use.

10. What is a Pseudorandom Number Generator (PRNG)?

A PRNG is an algorithm that generates a sequence of numbers that approximates random number properties. In cryptography, Cryptographically Secure PRNGs (CSPRNGs) are used for key generation and stream cipher keystreams. Example: BBS generator.

PART B – 16 Mark Questions

1. Explain the DES (Data Encryption Standard) algorithm in detail. Describe its structure, key generation, and each round of encryption with a neat diagram.

2. Explain the AES (Advanced Encryption Standard) algorithm. Describe its four transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey with examples.

3. Describe the Block Cipher Design Principles and Block Cipher Modes of Operation (ECB, CBC, CFB, OFB, CTR) with diagrams and comparison.

4. Explain Differential Cryptanalysis and Linear Cryptanalysis techniques. How do these attacks compromise DES security?

5. Describe the Evaluation Criteria for AES. Explain Pseudorandom Number Generators and RC4 stream cipher with its working and vulnerabilities.

UNIT III – ASYMMETRIC CRYPTOGRAPHY

PART A – 2 Mark Questions with Answers

1. What is Asymmetric Key Cryptography?

Asymmetric Key Cryptography (Public Key Cryptography) uses a pair of keys: a public key (shared openly) for encryption and a private key (kept secret) for decryption. Examples: RSA, Diffie-Hellman, ECC. It solves the key distribution problem.

2. What is the RSA Cryptosystem?

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem based on the difficulty of factoring large integers. It uses two keys: public key (e, n) for encryption and private key (d, n) for decryption. Security relies on the hardness of factoring n = p*q.

3. How does RSA Encryption work?

RSA Encryption: C = M^e mod n, where M is plaintext, e is public exponent, n is modulus. RSA Decryption: M = C^d mod n, where d is private exponent. Keys are generated using two large prime numbers p and q.

4. What is Key Distribution in Public Key Cryptography?

Key Distribution in public key cryptography involves securely sharing public keys. A Public Key Infrastructure (PKI) with Certificate Authorities (CAs) issues digital certificates to bind public keys to identities, solving the key distribution problem.

5. What is Key Management?

Key Management encompasses the generation, distribution, storage, rotation, and revocation of cryptographic keys. It ensures keys are available when needed, protected from unauthorized access, and retired when compromised or expired.

6. What is Diffie-Hellman Key Exchange?

Diffie-Hellman (DH) Key Exchange is a protocol that allows two parties to establish a shared secret key over an insecure channel without prior communication. It is based on the discrete logarithm problem. It does not provide encryption but enables key agreement.

7. What is Elliptic Curve Cryptography (ECC)?

ECC is a public-key cryptography approach based on the algebraic structure of elliptic curves over finite fields. It provides equivalent security to RSA with much smaller key sizes (256-bit ECC ≈ 3072-bit RSA), making it efficient for mobile and IoT devices.

8. What is Elliptic Curve Arithmetic?

Elliptic Curve Arithmetic involves operations on points of an elliptic curve: Point Addition (P + Q) and Point Doubling (P + P = 2P). These operations form a group structure used in key generation and ECDH key exchange and ECDSA digital signatures.

9. What is the difference between RSA and Diffie-Hellman?

RSA is used for both encryption and digital signatures; DH is only used for key exchange. RSA security is based on integer factorization; DH is based on discrete logarithm. RSA requires a trusted third party; DH provides perfect forward secrecy.

10. What are the advantages of ECC over RSA?

ECC advantages over RSA: (i) Smaller key sizes for equivalent security, (ii) Faster computation, (iii) Lower power consumption, (iv) Suitable for constrained devices (IoT, mobile). Disadvantage: more complex implementation than RSA.

PART B – 16 Mark Questions

1. Explain the RSA cryptosystem in detail. Describe key generation, encryption, decryption processes with a numerical example and its security analysis.

2. Explain the Diffie-Hellman Key Exchange protocol. Describe how two parties establish a shared secret and explain its vulnerability to man-in-the-middle attacks.

3. Describe Elliptic Curve Cryptography (ECC). Explain elliptic curve arithmetic, ECDH key exchange, and ECDSA. Compare ECC with RSA.

4. Explain Public Key Distribution methods. Describe Public Key Authority, Public Key Certificates, and Public Key Infrastructure (PKI) in detail.

5. Describe Key Management in asymmetric cryptography. Explain key generation, distribution, storage, and revocation using PKI and Certificate Authorities.

UNIT IV – INTEGRITY AND AUTHENTICATION ALGORITHMS

PART A – 2 Mark Questions with Answers

1. What is Authentication?

Authentication is the process of verifying the identity of a user, device, or entity. It ensures that entities are who they claim to be. Types: Something you know (password), Something you have (token), Something you are (biometrics).

2. What is a Hash Function?

A Hash Function is a mathematical function that maps an input of arbitrary length to a fixed-length output (hash/digest). Properties: Deterministic, fast computation, pre-image resistance, collision resistance. Examples: MD5 (128-bit), SHA-1 (160-bit), SHA-256.

3. What is a MAC (Message Authentication Code)?

A MAC is a short piece of information used to authenticate a message and provide integrity assurance. It is computed using a secret key and the message: MAC = f(K, M). The receiver verifies integrity by recomputing the MAC. Example: HMAC.

4. What is HMAC?

HMAC (Hash-based Message Authentication Code) is a MAC that uses a cryptographic hash function (like SHA-256) combined with a secret key. HMAC = H((K XOR opad) || H((K XOR ipad) || M)). It provides both authentication and data integrity.

5. What is CMAC?

CMAC (Cipher-based Message Authentication Code) is a MAC algorithm based on a block cipher (AES). It processes the message in blocks and produces a fixed-size authentication tag. CMAC is standardized by NIST and used where AES is already deployed.

6. What is SHA (Secure Hash Algorithm)?

SHA (Secure Hash Algorithm) is a family of cryptographic hash functions by NIST. SHA-1 produces 160-bit digest (now deprecated). SHA-2 family (SHA-256, SHA-512) is widely used. SHA-3 uses Keccak sponge construction. Used for digital signatures and integrity.

7. What is Entity Authentication?

Entity Authentication is the process of verifying the identity of a communicating party in real-time. Unlike data origin authentication, it proves the entity is live and actively participating. Methods include passwords, challenge-response protocols, biometrics.

8. What is a Challenge-Response Protocol?

A Challenge-Response Protocol proves identity without revealing the secret. The verifier sends a random challenge; the claimant computes a response using their secret key. The verifier validates the response. This prevents replay attacks. Example: CHAP.

9. What is Kerberos?

Kerberos is a network authentication protocol that uses symmetric key cryptography and a trusted third party (Key Distribution Center - KDC) to authenticate users to services. It provides SSO and mutual authentication. Used in Windows Active Directory environments.

10. What are Biometrics in Authentication?

Biometrics use unique physical or behavioral characteristics for authentication: fingerprint, iris scan, facial recognition, voice recognition, and retina scan. They provide strong authentication since biometric traits are difficult to forge or steal, unlike passwords.

PART B – 16 Mark Questions

1. Explain the SHA (Secure Hash Algorithm) family in detail. Describe SHA-1 and SHA-256 algorithms, their structure, and security analysis.

2. Describe HMAC and CMAC in detail. Explain their construction, working, and how they provide message authentication and integrity.

3. Explain Entity Authentication methods: Passwords, Biometrics, and Challenge-Response Protocols. Compare their security and usability.

4. Describe the Kerberos Authentication Protocol in detail. Explain the roles of KDC, TGS, and the ticket-based authentication process with a diagram.

5. Explain Hash Functions and their properties. Describe the security of hash functions and discuss birthday attacks and collision resistance.

UNIT V – CYBER CRIMES AND CYBER SECURITY

PART A – 2 Mark Questions with Answers

1. What is Cyber Crime?

Cyber Crime refers to criminal activities carried out using computers, networks, or the internet. It includes unauthorized access, data theft, fraud, cyberbullying, identity theft, and distribution of malware. Cyber crimes

target individuals, organizations, and governments.

2. What are the classifications of Cyber Crimes?

Cyber Crimes are classified as: (i) Crimes against individuals (hacking, stalking), (ii) Crimes against property (data theft, vandalism), (iii) Crimes against organizations (corporate espionage), and (iv) Crimes against society/government (cyber terrorism, spreading misinformation).

3. What is Password Cracking?

Password Cracking is the process of recovering passwords from stored or transmitted data. Techniques include: Brute Force (try all combinations), Dictionary Attack (use word lists), Rainbow Table Attack (precomputed hashes), and Phishing. Tools: John the Ripper, Hashcat.

4. What is a Keylogger?

A Keylogger is malware that records keystrokes made by a user to steal sensitive information like passwords, credit card numbers, and messages. Keyloggers can be software-based (programs) or hardware-based (physical devices attached to keyboard). Detected by anti-malware software.

5. What is Spyware?

Spyware is malicious software that secretly monitors user activity, collects sensitive information (browsing history, passwords, financial data), and sends it to a third party without user consent. It is installed without the user's knowledge, often bundled with free software.

6. What is SQL Injection?

SQL Injection is a web security vulnerability where an attacker injects malicious SQL code into input fields of a web application to manipulate the backend database. It can expose, modify, or delete data. Prevention: Use parameterized queries and prepared statements.

7. What is Network Access Control (NAC)?

Network Access Control (NAC) is a security solution that enforces policies on devices seeking to access a network. It checks device health, user identity, and compliance before granting access. It prevents unauthorized devices from connecting to the network.

8. What is Cloud Security?

Cloud Security refers to policies, technologies, and controls to protect cloud data, applications, and infrastructure from threats. It addresses shared responsibility, data breaches, insecure APIs, account hijacking, and compliance issues. Tools: CASB, IAM, encryption.

9. What is Web Security?

Web Security protects websites and web applications from attacks such as XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), SQL Injection, and clickjacking. It includes HTTPS, input validation, Content Security Policy (CSP), and web application firewalls (WAF).

10. What is Wireless Security?

Wireless Security protects wireless networks from unauthorized access and attacks. It includes protocols like WEP (deprecated), WPA, WPA2, and WPA3. Threats include eavesdropping, rogue access points, and de-authentication attacks. Best practice: Use WPA3 with strong passwords.

PART B – 16 Mark Questions

1. Explain Cyber Crimes and Cyber Security in detail. Describe the classifications of cyber crimes and the tools and methods used by cybercriminals.

2. Explain Password Cracking, Keyloggers, and Spyware. Describe how these tools work, their impact, and countermeasures to prevent them.

3. Describe SQL Injection attack in detail. Explain types of SQL injection, how attackers exploit it, and methods to prevent SQL injection vulnerabilities.

4. Explain Network Access Control (NAC), Cloud Security, and Web Security. Describe the threats and security mechanisms for each.

5. Write a detailed note on Wireless Security. Explain WEP, WPA, WPA2, and WPA3 protocols, their vulnerabilities, and best practices for securing wireless networks.

— End of Question Bank — U23CBT43 Cryptography and Cyber Security —