Network Security and Cryptography (23CY501)

Tutorial Sheet – Unit I

Security Concepts and Cryptography Concepts & Techniques

Part A: Short Answer Questions

1. Define information security.
2. Why is security important in computer networks?
3. Explain the CIA triad.
4. What is meant by confidentiality?
5. Differentiate between active and passive attacks.
6. Define authentication and authorization.
7. What are security services?
8. List the major security mechanisms.
9. Explain the network security model.
10. Define cryptography.
11. What is plaintext?
12. What is ciphertext?
13. Differentiate between encryption and decryption.
14. What is a cryptographic key?
15. Define steganography.
16. What is symmetric key cryptography?
17. What is asymmetric key cryptography?
18. What is key size?
19. What is key range?
20. List different types of cryptographic attacks.

Part B: Descriptive Questions

Security Concepts

1. Explain the need for security in modern communication systems.
2. Discuss various security approaches used in computer networks.
3. Explain the principles of security with suitable examples.
4. Compare active attacks and passive attacks.
5. Explain different types of security attacks in detail.
6. Discuss the security services provided by network security systems.
7. Explain the various security mechanisms with examples.
8. Describe the model for network security with a neat diagram.

Cryptography Concepts

9. Explain the process of encryption and decryption.
10. Differentiate between plaintext and ciphertext.
11. Compare substitution techniques and transposition techniques.
12. Explain symmetric key cryptography with advantages and disadvantages.
13. Explain asymmetric key cryptography with suitable examples.
14. Compare symmetric and asymmetric cryptographic systems.
15. Explain steganography and compare it with cryptography.
16. Discuss key size and key range and their importance in security.
17. Explain different possible attacks on cryptographic systems.
18. Describe the role of cryptography in ensuring confidentiality and integrity.

Part C: Analytical Questions

1. Why are passive attacks difficult to detect while active attacks are easier to detect?
2. If confidentiality is maintained but integrity is compromised, what problems may arise?
3. Analyze the advantages and disadvantages of symmetric key encryption.
4. Why is asymmetric encryption generally slower than symmetric encryption?
5. Compare cryptography and steganography in terms of security and practicality.
6. How does increasing key size improve security?
7. Explain why brute-force attacks become difficult with larger key sizes.
8. Discuss how multiple security services work together to secure a network.

Part D: Problem-Solving Exercises

Substitution Cipher

1. Encrypt the plaintext **"HELLO"** using a Caesar Cipher with shift = 3.
2. Decrypt the ciphertext **"KHOOR"** using a Caesar Cipher.
3. Encrypt the word **"SECURITY"** using a Caesar Cipher with shift = 5.
4. Perform encryption using a monoalphabetic substitution cipher with a given key mapping.

Transposition Cipher

5. Apply columnar transposition on the plaintext **"NETWORKSECURITY"** using the key **3142**.
6. Decrypt a given columnar transposition ciphertext.

Symmetric and Asymmetric Cryptography

7. Explain the steps involved in symmetric key encryption between two users.
8. Illustrate public key encryption using a simple example.
9. Show how a sender encrypts a message using the receiver's public key.
10. Explain how digital signatures provide authentication.

Part E: Multiple Choice Questions (MCQs)

1. The primary goal of confidentiality is:
    - A) Prevent unauthorized modification
    - B) Prevent unauthorized disclosure
    - C) Prevent service interruption
    - D) Improve performance

    Answer: B
2. Which of the following is a passive attack?
    - A) Masquerade
    - B) Replay
    - C) Eavesdropping
    - D) Modification

    Answer: C
3. Encryption converts:
    - A) Ciphertext into plaintext
    - B) Plaintext into ciphertext
    - C) Key into plaintext
    - D) Ciphertext into key

    Answer: B
4. AES is an example of:
    - A) Asymmetric encryption
    - B) Symmetric encryption
    - C) Hashing
    - D) Steganography

    Answer: B
5. RSA is an example of:
    - A) Symmetric algorithm
    - B) Stream cipher
    - C) Asymmetric algorithm
    - D) Hash function

    Answer: C
6. The process of hiding information inside another medium is called:
    - A) Encryption
    - B) Decryption
    - C) Steganography
    - D) Authentication

    Answer: C

7. A brute-force attack attempts:
    - A) Social engineering
    - B) Guessing all possible keys
    - C) Packet filtering
    - D) Compression

    Answer: B
8. Integrity ensures:
    - A) Data secrecy
    - B) Data accuracy and completeness
    - C) Data availability
    - D) Key management

    Answer: B

Part F: Assignment Questions

1. Prepare a report on real-world cyber attacks and classify them as active or passive attacks.
2. Compare AES and RSA algorithms.
3. Study the role of cryptography in online banking systems.
4. Analyze the impact of key length on cryptographic security.
5. Demonstrate Caesar Cipher and Columnar Transposition Cipher using examples.
6. Investigate modern steganography techniques and applications.

Viva Questions

1. What is the difference between security and privacy?
2. What are the three pillars of information security?
3. Explain active and passive attacks with examples.
4. What is ciphertext?
5. What is a cryptographic key?
6. Differentiate between symmetric and asymmetric encryption.
7. What is steganography?
8. What is a brute-force attack?
9. Why is key size important?
10. Explain the network security model.