# Network Security and Cryptography (23CY501)

**Tutorial Sheet – Unit III**
**Cryptographic Hash Functions, Message Authentication, Digital Signatures, Key Management and Distribution**

**Part A: Short Answer Questions**
**Cryptographic Hash Functions**

1. Define a cryptographic hash function.
2. What is message authentication?
3. What are the requirements of message authentication?
4. Define a hash value (digest).
5. What is collision resistance?
6. What is pre-image resistance?
7. Expand SHA.
8. What is SHA-512?
9. State the output size of SHA-512.
10. List the properties of a secure hash function.

**Message Authentication Codes**

11. What is a Message Authentication Code (MAC)?
12. Define HMAC.
13. Expand HMAC.
14. What is CMAC?
15. Expand CMAC.
16. Differentiate between HMAC and CMAC.
17. What is the purpose of MAC in communication?

**Digital Signatures**

18. Define a digital signature.
19. What are the objectives of digital signatures?
20. What is non-repudiation?
21. What is signature verification?
22. What is the ElGamal Digital Signature Scheme?
23. Differentiate between encryption and digital signature.

**Key Management and Distribution**

24. What is key management?
25. What is key distribution?
26. Explain symmetric key distribution.
27. Explain public key distribution.
28. What is Kerberos?

29. What is a ticket in Kerberos?
30. What is X.509 authentication?
31. What is a digital certificate?
32. What is Public Key Infrastructure (PKI)?
33. What is a Certificate Authority (CA)?
34. What is certificate revocation?

**Part B: Long Answer Questions**

**Cryptographic Hash Functions**

1. Explain the concept of message authentication and its requirements.
2. Discuss the characteristics of cryptographic hash functions.
3. Explain the structure and working of SHA-512.
4. Describe the SHA-512 algorithm with a neat diagram.
5. Discuss the applications of cryptographic hash functions in network security.
6. Explain collision resistance, pre-image resistance, and second pre-image resistance.

**Message Authentication Codes**

7. Explain Message Authentication Codes (MACs) and their importance.
8. Describe the working of HMAC with a neat diagram.
9. Explain the HMAC generation and verification process.
10. Discuss the CMAC algorithm and its operation.
11. Compare HMAC and CMAC.
12. Explain how message authentication is achieved using MACs.

**Digital Signatures**

13. Explain digital signatures and their security services.
14. Describe the process of digital signature generation and verification.
15. Explain the ElGamal Digital Signature Scheme with a suitable example.
16. Discuss the advantages and limitations of digital signatures.
17. Compare MACs and Digital Signatures.
18. Explain how digital signatures provide authentication, integrity, and non-repudiation.

**Key Management and Distribution**

19. Explain symmetric key distribution using symmetric encryption.
20. Explain symmetric key distribution using asymmetric encryption.
21. Discuss various methods of public key distribution.
22. Explain the working of Kerberos authentication service.
23. Describe the architecture and operation of Kerberos.
24. Explain the X.509 Authentication Service in detail.

25. Discuss the format and contents of an X.509 certificate.
26. Explain Public Key Infrastructure (PKI) and its components.
27. Describe the role of Certificate Authorities in PKI.
28. Compare Kerberos and PKI.
29. Explain key management challenges in secure communication systems.
30. Discuss the importance of certificate management in PKI.

**Part C: Analytical and Conceptual Questions**

1. Why are cryptographic hash functions considered one-way functions?
2. Analyze the role of SHA-512 in ensuring data integrity.
3. Why is HMAC more secure than a simple hash function for authentication?
4. Compare HMAC and digital signatures.
5. Why is non-repudiation not provided by MACs?
6. Discuss the importance of digital signatures in e-commerce.
7. Analyze the advantages of Kerberos in network authentication.
8. Why is PKI necessary in large-scale networks?
9. Compare symmetric and asymmetric key distribution methods.
10. Explain the importance of Certificate Authorities in trust management.

**Part D: Problem-Solving and Application Questions**

**Hash Functions**

1. Explain how SHA-512 processes a message block.
2. Demonstrate the steps involved in generating a hash value.
3. Explain how hash functions detect message modification.

**HMAC and CMAC**

4. Illustrate the HMAC generation process using a simple example.
5. Explain the verification process of HMAC.
6. Compare the working of HMAC and CMAC using a suitable example.

**Digital Signatures**

7. Draw and explain the digital signature generation process.
8. Draw and explain the digital signature verification process.
9. Explain the ElGamal Digital Signature Scheme with a numerical example.
10. Demonstrate how digital signatures ensure non-repudiation.

**Kerberos and PKI**

11. Draw the architecture of Kerberos and explain its operation.
12. Illustrate the ticket-granting process in Kerberos.
13. Explain the certificate issuance process in PKI.
14. Draw the structure of an X.509 certificate and explain its fields.
15. Demonstrate how public keys are distributed using PKI.

**Part E: Multiple Choice Questions (MCQs)**

1. SHA-512 produces a digest of:
    - A) 128 bits
    - B) 256 bits
    - C) 512 bits
    - D) 1024 bits

    **Answer:** C
2. HMAC stands for:
    - A) Hash Message Authentication Code
    - B) Hyper Message Authentication Code
    - C) Host Message Access Control
    - D) Hash Media Access Control

    **Answer:** A
3. CMAC is based on:
    - A) Hash functions
    - B) Block ciphers
    - C) Stream ciphers
    - D) Digital signatures

    **Answer:** B
4. A digital signature provides:
    - A) Compression
    - B) Authentication
    - C) Routing
    - D) Multiplexing

    **Answer:** B
5. Non-repudiation means:
    - A) Data confidentiality
    - B) Data availability
    - C) Sender cannot deny sending the message
    - D) Encryption **Answer:** C

6. Kerberos uses:
    - A) Certificate Authority
    - B) Trusted Third Party
    - C) Router
    - D) Firewall

    **Answer:** B
7. X.509 is a standard for:
    - A) Routing
    - B) Digital Certificates
    - C) Hash Functions
    - D) Encryption

    **Answer:** B
8. PKI stands for:
    - A) Private Key Infrastructure
    - B) Public Key Integration
    - C) Public Key Infrastructure
    - D) Protected Key Infrastructure

    **Answer:** C
9. The trusted entity in PKI is:
    - A) DNS Server
    - B) Certificate Authority
    - C) Switch
    - D) Proxy

    **Answer:** B
10. SHA-512 belongs to the:
    - A) SHA-2 family
    - B) SHA-1 family
    - C) DES family
    - D) RSA family

    **Answer:** A



**Part F: Assignment Questions**

1. Study the working of SHA-512 and prepare a report on its applications.
2. Compare SHA-256 and SHA-512 in terms of security and performance.
3. Analyze the role of HMAC in securing web applications.
4. Study digital signatures used in e-governance systems.
5. Implement a simple message authentication mechanism using hashing.

6. Investigate the ElGamal Digital Signature Scheme and its applications.
7. Study the Kerberos authentication protocol and prepare a flow diagram.
8. Analyze the architecture and components of PKI.
9. Study X.509 certificates used in HTTPS websites.
10. Compare Kerberos and PKI-based authentication systems.

**Viva Questions**

1. What is a cryptographic hash function?
2. What is SHA-512?
3. What is a message digest?
4. What is HMAC?
5. What is CMAC?
6. What is message authentication?
7. What is a digital signature?
8. What is non-repudiation?
9. What is the ElGamal Digital Signature Scheme?
10. What is key management?
11. What is key distribution?
12. What is Kerberos?
13. What is a Ticket Granting Server (TGS)?
14. What is an X.509 certificate?
15. What is PKI?
16. What is a Certificate Authority?
17. How are public keys distributed?
18. What is certificate revocation?
19. What is the difference between HMAC and Digital Signature?
20. Why is PKI important in secure communication?

**Important University Exam Questions (Frequently Asked)**

1. Explain SHA-512 algorithm with a neat diagram.
2. Discuss message authentication and authentication requirements.
3. Explain HMAC and CMAC.
4. Describe digital signatures and ElGamal Digital Signature Scheme.
5. Explain symmetric and asymmetric key distribution techniques.
6. Discuss public key distribution methods.
7. Explain Kerberos authentication service with architecture.