Cryptography and Network Security

Question Paper - 2022

Part A (8 × 6 = 48 marks)

1. Define and explain the OSI Security Architecture.
2. Describe substitution and transposition techniques with examples.
3. Explain the principles of block cipher design.
4. Differentiate between DES and AES.
5. State and prove Euler's theorem.
6. What is a Message Authentication Code (MAC)? Give an example.
7. Describe Kerberos and its significance in authentication.
8. Explain the purpose and architecture of IP Security.

Part B (7 × 10 = 70 marks)

1. a) Compare symmetric and asymmetric encryption.
   b) Explain classical encryption techniques with examples.
2. a) Explain the structure and working of the DES algorithm.
   b) Describe multiple encryption and Triple DES.
3. a) Describe the RSA algorithm with an example.
   b) Explain Chinese Remainder Theorem and its application in cryptography.
4. a) Discuss Hash Functions and their properties.
   b) Describe the Digital Signature Standard (DSS).
5. a) What is X.509 Authentication Service?
   b) Explain the concept of Public Key Infrastructure.
6. a) Discuss SSL/TLS protocol in web security.
   b) Describe intrusion detection techniques.
7. a) Write a note on firewall types and design principles.
   b) Explain password management techniques in secure systems.

Question Paper - 2023

Part A (8 × 6 = 48 marks)

1. Explain security services and security mechanisms.
2. What is steganography? How is it different from cryptography?
3. Illustrate AES structure with simplified AES example.
4. Define stream cipher and explain RC4 algorithm.
5. What is the role of Fermat's theorem in RSA?
6. Discuss authentication requirements in secure systems.
7. What is the role of Encapsulating Security Payload (ESP)?
8. Describe the architecture of a firewall.

Part B (7 × 10 = 70 marks)

1. a) Describe the symmetric cipher model.
   b) Explain various types of security attacks.
2. a) Explain differential and linear cryptanalysis.
   b) Describe block cipher modes of operation.
3. a) Discuss the Diffie-Hellman key exchange algorithm.
   b) Explain Elliptic Curve Cryptography with advantages.
4. a) Compare Hash functions and Message Authentication Codes (MACs).
   b) Discuss the security of hash functions.
5. a) Explain authentication header in IP security.
   b) Describe key management in IPsec.
6. a) What are digital signatures? Explain with examples.
   b) Describe Kerberos working and use case.
7. a) Explain intrusion detection systems and their classification.
   b) Write a note on web security threats and countermeasures.

Question Paper - 2024

Part A (8 × 6 = 48 marks)

1. Write a note on the model for network security.
2. Describe transposition techniques with an example.
3. Explain the structure of AES and GF(2^8) arithmetic.
4. What is triple DES and when is it used?
5. State and explain the Chinese Remainder Theorem.
6. What is digital signature? State its importance.
7. Describe Secure Socket Layer (SSL) architecture.
8. Explain the concept of intrusion and password management.

Part B (7 × 10 = 70 marks)

1. a) Describe classical symmetric encryption techniques.
   b) Explain the security trends in modern networks.
2. a) Discuss the working of AES encryption in detail.
   b) Differentiate between stream cipher and block cipher.
3. a) Explain RSA key generation and encryption/decryption.
   b) Describe elliptic curve arithmetic.
4. a) Explain authentication functions and types.
   b) What are MACs? Give a suitable example.
5. a) Describe the structure and components of IPsec.
   b) Explain security associations and how they are combined.
6. a) Discuss X.509 and its role in authentication.
   b) Describe PKI and its application in secure communication.
7. a) Explain the architecture and working of SSL/TLS.
   b) What are firewalls? How do they help in preventing attacks?