Short Questions

1. What is the main purpose of security in computing?
2. Name three reasons why security is essential in computing systems.
3. Define "security approaches" and provide examples of different approaches.
4. List three principles of security.
5. Describe the difference between passive and active security attacks.
6. What are the primary security services provided by secure systems?
7. Provide examples of security mechanisms used to protect systems.
8. Explain the components of a model for network security.
9. Why is cryptography important in ensuring data security?
10. Define plaintext and ciphertext.
11. What is the purpose of substitution techniques in cryptography?
12. Give an example of a substitution technique.
13. Describe transposition techniques in cryptography.
14. How does encryption differ from decryption?
15. Differentiate between symmetric and asymmetric key cryptography.
16. What is steganography, and how is it used in security?
17. Explain the significance of key range and key size in cryptography.
18. List common types of attacks that can compromise cryptographic systems.
19. Define the term "vulnerability" in the context of security.
20. What role do security policies play in ensuring system security?
21. Describe the concept of access control and its importance in security.
22. What is authentication, and why is it crucial in secure systems?
23. Explain the difference between confidentiality and integrity in security.
24. How does encryption contribute to achieving confidentiality?
25. Define "firewall" and its function in network security.

26. What are intrusion detection systems (IDS), and how do they enhance security?
27. Describe the principle of least privilege and its significance in security.
28. Explain the concept of encryption key management.
29. What is the difference between a virus and a worm in terms of security threats?
30. Define "denial-of-service (DoS)" attacks and their impact on systems.
31. What role do security audits play in maintaining system security?
32. Explain the concept of risk management in security.
33. Define "social engineering" and its relevance to security.
34. Describe the importance of user awareness training in security measures.
35. What is the significance of encryption algorithms in cryptography?
36. Define "hash function" and its application in security.
37. Explain how digital signatures contribute to authentication in secure communication.
38. Describe the role of public key infrastructure (PKI) in asymmetric cryptography.
39. What is the difference between a threat and a vulnerability in security terminology?
40. Explain the concept of multi-factor authentication (MFA).
41. Describe the process of key exchange in cryptographic protocols.
42. What is the role of digital certificates in establishing trust in online transactions?
43. Define the term "non-repudiation" in the context of security.
44. How do security patches contribute to maintaining system security?
45. Explain the concept of network segmentation and its impact on security.
46. Describe the importance of encryption in securing data at rest.
47. What are the challenges associated with securing cloud-based systems?

48. Define "end-to-end encryption" and its importance in secure communication.
49. How does biometric authentication enhance security measures?
50. Explain the concept of security through obscurity and its limitations in practice.
51. What are the fundamental principles of block ciphers?
52. Explain the operation of a block cipher.
53. Describe the Data Encryption Standard (DES) and its key characteristics.
54. What is the Advanced Encryption Standard (AES), and why is it significant?
55. Discuss the features and usage of the Blowfish cipher.
56. Explain the structure and operation of the RC5 cipher.
57. Describe the IDEA cipher and its strengths in encryption.
58. How do block cipher modes of operation enhance encryption?
59. Define stream ciphers and provide an example.
60. Explain the operation of the RC4 stream cipher.
61. What are the key principles of public-key cryptosystems?
62. Describe the RSA algorithm and its key components.
63. Explain the concept of ElGamal cryptography and its applications.
64. How does the Diffie-Hellman Key Exchange protocol work?
65. Discuss the Knapsack Algorithm and its role in cryptography.
66. Define cryptographic hash functions and their purpose.
67. Explain the concept of message authentication using hash functions.
68. Describe the Secure Hash Algorithm (SHA-512) and its properties.
69. What are message authentication codes (MACs), and why are they used?
70. Discuss the HMAC (Hash-based Message Authentication Code) construction.
71. Explain the CMAC (Cipher-based Message Authentication Code) algorithm.

72. What are digital signatures, and how do they provide authenticity?
73. Describe the ElGamal Digital Signature Scheme and its components.
74. How does the choice of block size affect the security of a block cipher?
75. What are the key differences between symmetric and asymmetric key ciphers?
76. Explain why key management is crucial in symmetric key cryptography.
77. Describe the process of key generation in the RSA algorithm.
78. What role does the Euler's totient function play in RSA key generation?
79. How does the concept of prime factorization contribute to RSA security?
80. Discuss the concept of key distribution in asymmetric key cryptography.
81. Explain the concept of a digital envelope in asymmetric cryptography.
82. What is the significance of the Chinese Remainder Theorem in RSA decryption?
83. How does the security of ElGamal cryptography rely on the Discrete Logarithm Problem?
84. Describe the process of key exchange using the Diffie-Hellman protocol.
85. Discuss the advantages and disadvantages of symmetric and asymmetric key cryptography.
86. Explain the concept of key exchange vulnerability in symmetric key systems.
87. What are the main factors considered when selecting a cryptographic algorithm?
88. Describe the importance of key length in cryptographic algorithms.
89. How does the Avalanche effect contribute to the security of cryptographic algorithms?
90. Discuss the relevance of diffusion and confusion in block cipher design.
91. Explain why the use of a random initialization vector (IV) is crucial in block cipher modes.
92. What are the main properties of a secure cryptographic hash function?

93. How does a collision attack differ from a preimage attack in hash functions?
94. Discuss the role of salt in password hashing for secure storage.
95. Explain the concept of birthday attacks in cryptographic hash functions.
96. Describe the role of digital signatures in ensuring non-repudiation.
97. How does the RSA algorithm ensure the confidentiality of transmitted messages?
98. Discuss the role of padding in ensuring the security of RSA encryption.
99. What is the significance of the Chinese Remainder Theorem in RSA decryption?
100. Describe the security considerations when using hash functions for digital signatures.
101. How does the time complexity of the Knapsack Algorithm affect its security?
102. Discuss the importance of collision resistance in cryptographic hash functions.
103. Explain how HMAC enhances the security of message authentication.
104. What role does the key derivation function (KDF) play in cryptographic systems?
105. Discuss the importance of entropy in generating secure cryptographic keys.
106. Explain the concept of key stretching and its relevance to password hashing.
107. Describe the role of digital certificates in verifying public keys.
108. Discuss the security implications of using weak cryptographic algorithms.
109. What is the significance of the prime number selection process in RSA?
110. Explain how digital signatures provide message integrity.
111. Discuss the role of salt in password-based key derivation.

112.How does the concept of forward secrecy enhance cryptographic protocols?

113.Explain why the security of cryptographic algorithms relies on computational complexity.

114.What is the role of a nonce in cryptographic protocols?

115.Describe the process of key exchange using the RSA algorithm.

116.Discuss the importance of randomness in cryptographic systems.

117.How does the Diffie-Hellman protocol prevent eavesdropping in key exchange?

118.Explain the concept of cryptographically secure pseudorandom number generators (CSPRNGs).

119.Discuss the role of modular arithmetic in asymmetric key cryptography.

120.What are the advantages and disadvantages of using a block cipher over a stream cipher?

121.Explain why the key size is a critical factor in the security of cryptographic algorithms.

122.Discuss the security considerations when implementing cryptographic protocols.

123.What are the main challenges in securely distributing cryptographic keys?

124.Describe the concept of Perfect Forward Secrecy (PFS) in cryptographic systems.

125.How does quantum computing pose a threat to current cryptographic systems, and what solutions are being explored to address this threat?