1. Which cryptographic technique ensures the integrity and authenticity of a message by

appending a unique code generated with a private key?

- a) Message Authentication Code (MAC)
- b) Digital Signature
- c) Hash Function
- d) Key Exchange

Answer: b) Digital Signature

Explanation: Digital signatures use asymmetric cryptography to sign messages with a private key, allowing recipients to verify the authenticity and integrity using the corresponding public key.

- 2. What is the primary purpose of a digital signature?
- a) Encryption
- b) Authentication
- c) Compression
- d) Decryption

Answer: b) Authentication

Explanation: Digital signatures primarily serve to authenticate the sender of a message and ensure the integrity of the transmitted data.

3. Which cryptographic technique is used to securely distribute encryption keys between parties?

- a) Message Authentication
- b) Digital Signature
- c) Key Management

d) Key Exchange

Answer: d) Key Exchange

Explanation: Key exchange protocols facilitate the secure distribution of cryptographic keys between communicating parties to establish a shared secret key for encrypted communication.

4. Which type of hashing algorithm is designed to minimize the likelihood of collisions by using a randomization technique?

- a) Universal Hashing
- b) Cryptographic Hash Function
- c) MD Hash Function
- d) Secure Hash Algorithm (SHA)

Answer: a) Universal Hashing

Explanation: Universal hashing involves randomly selecting a hash function from a family of hash functions, reducing the probability of collisions.

5. Which cryptographic hash function is widely used for its security and resistance to collision attacks?

- a) MD5
- b) SHA-1
- c) SHA-256
- d) SHA-512

Answer: c) SHA-256

Explanation: SHA-256 is part of the SHA-2 family of cryptographic hash functions and is

known for its security and resistance to collision attacks.

6. Which cryptographic attack exploits the trade-off between memory and computation to reduce the time complexity of breaking a cipher?

- a) Differential Cryptanalysis
- b) Time-Memory Trade-off Attack
- c) Birthday Attack
- d) Chosen-Plaintext Attack

Answer: b) Time-Memory Trade-off Attack

Explanation: Time-memory trade-off attacks exploit the trade-off between computation and memory usage to reduce the time complexity of cryptographic attacks.

7. Which cryptographic standard is used for digital signatures in the US government and other applications requiring high levels of security?

- a) Message Digest (MD)
- b) Digital Signature Standard (DSS)
- c) Data Encryption Standard (DES)
- d) Advanced Encryption Standard (AES)

Answer: b) Digital Signature Standard (DSS)

Explanation: DSS is a standard for digital signatures, specified by the National Institute of Standards and Technology (NIST) in the United States.

8. Which cryptographic attack focuses on analyzing the differences in input and output of a cryptographic algorithm to break its security?

a) Time-Memory Trade-off Attack

- b) Differential Cryptanalysis
- c) Birthday Attack
- d) Meet-in-the-Middle Attack

Answer: b) Differential Cryptanalysis

Explanation: Differential cryptanalysis involves studying the differences in the input and output of a cryptographic algorithm to exploit patterns and break its security.

9. Which cryptographic system provides secure authentication for network services by using tickets and a trusted third party?

- a) RSA
- b) AES
- c) Kerberos
- d) SSL/TLS

Answer: c) Kerberos

Explanation: Kerberos is a network authentication protocol that provides secure authentication by using tickets and a trusted third-party authentication server.

10. What is the primary function of a hash function in cryptography?

- a) Encryption
- b) Compression
- c) Authentication
- d) Key Exchange

Answer: c) Authentication

Explanation: Hash functions are primarily used for authentication purposes, ensuring the

integrity and authenticity of data by generating fixed-size hash values.

11. Which cryptographic algorithm is vulnerable to length extension attacks and is no longer considered secure for cryptographic purposes?

- a) MD5
- b) SHA-1
- c) SHA-256
- d) SHA-512

Answer: a) MD5

Explanation: MD5 is vulnerable to length extension attacks and is no longer considered secure for cryptographic purposes due to its susceptibility to collisions.

12. Which cryptographic technique involves the use of symmetric keys to ensure the integrity and authenticity of transmitted data?

- a) Digital Signature
- b) Message Authentication Code (MAC)
- c) Key Exchange
- d) Public Key Infrastructure (PKI)

Answer: b) Message Authentication Code (MAC)

Explanation: MACs use symmetric keys to generate authentication tags for verifying the integrity and authenticity of transmitted data.

13. Which cryptographic technique ensures the confidentiality of data by converting it into an unreadable format using a secret key?a) Hash Function

- b) Digital Signature
- c) Encryption
- d) Key Exchange

Answer: c) Encryption

Explanation: Encryption involves converting plaintext into ciphertext using a secret key, ensuring the confidentiality of data.

- 14. What is the primary objective of key management in cryptography?
- a) Ensuring message integrity
- b) Facilitating secure communication
- c) Managing cryptographic keys securely
- d) Preventing cryptographic attacks

Answer: c) Managing cryptographic keys securely

Explanation: Key management involves the secure generation, distribution, storage, and destruction of cryptographic keys to ensure the security of cryptographic systems.

15. Which cryptographic attack exploits the probability of two different inputs producing the same hash output?

- a) Birthday Attack
- b) Chosen-Plaintext Attack
- c) Differential Cryptanalysis
- d) Side-Channel Attack

Answer: a) Birthday Attack

Explanation: Birthday attacks exploit the probability of collisions in hash functions, where two

different inputs produce the same hash output.

16. Which cryptographic standard specifies the use of SHA-2 for secure hash functions?

- a) Digital Signature Standard (DSS)
- b) Data Encryption Standard (DES)
- c) Advanced Encryption Standard (AES)
- d) Secure Hash Algorithm (SHA)

Answer: a) Digital Signature Standard (DSS)

Explanation: DSS specifies the use of SHA-2 (including SHA-256, SHA-384, and SHA-512) for secure hash functions in digital signatures.

17. Which cryptographic attack focuses on exploiting weaknesses in the generation of random numbers in cryptographic systems?

- a) Birthday Attack
- b) Differential Cryptanalysis
- c) Side-Channel Attack
- d) Random Number Generation Attack

Answer: d) Random Number Generation Attack

Explanation: Random number generation attacks exploit weaknesses in the generation of random numbers in cryptographic systems to compromise their security.

18. Which cryptographic algorithm is widely used for symmetric-key encryption and decryption?

- a) RSA
- b) AES

c) ECC d) Diffie-Hellman

Answer: b) AES

Explanation: Advanced Encryption Standard (AES) is widely used for symmetric-key encryption and decryption due to its efficiency and security.

19. Which cryptographic technique involves the use of mathematical functions to convert data into a fixed-size string of bytes?

- a) Digital Signature
- b) Message Authentication Code (MAC)
- c) Hash Function
- d) Key Exchange

Answer: c) Hash Function

Explanation: Hash functions are mathematical functions used to convert data into a fixed-size string of bytes, ensuring data integrity and authenticity.

20. Which cryptographic protocol provides secure communication over an insecure network through encryption, authentication, and integrity protection?

- a) SSH
- b) HTTP
- c) FTP
- d) SSL/TLS

Answer: a) SSH

Explanation: Secure Shell (SSH) protocol provides secure communication over an insecure

network through encryption, authentication, and integrity protection.

Related posts:

- 1. Mathematical Background for Cryptography MCQ
- 2. Cryptography MCQ
- 3. Information Security MCQ
- 4. Cryptography and Information Security Tools MCQ
- 5. Introduction to Energy Science MCQ
- 6. Ecosystems MCQ
- 7. Biodiversity and its conservation MCQ
- 8. Environmental Pollution mcq
- 9. Social Issues and the Environment MCQ
- 10. Field work mcq
- 11. Discrete Structure MCQ
- 12. Set Theory, Relation, and Function MCQ
- 13. Propositional Logic and Finite State Machines MCQ
- 14. Graph Theory and Combinatorics MCQ
- 15. Relational algebra, Functions and graph theory MCQ
- 16. Data Structure MCQ
- 17. Stacks MCQ
- 18. TREE MCQ
- 19. Graphs MCQ
- 20. Sorting MCQ
- 21. Digital Systems MCQ
- 22. Combinational Logic MCQ
- 23. Sequential logic MCQ

- 24. Analog/Digital Conversion, Logic Gates, Multivibrators, and IC 555 MCQ
- 25. Introduction to Digital Communication MCQ
- 26. Introduction to Object Oriented Thinking & Object Oriented Programming MCQ
- 27. Encapsulation and Data Abstraction MCQ
- 28. MCQ
- 29. Relationships Inheritance MCQ
- 30. Polymorphism MCQ
- 31. Library Management System MCQ
- 32. Numerical Methods MCQ
- 33. Transform Calculus MCQ
- 34. Concept of Probability MCQ
- 35. Algorithms, Designing MCQ
- 36. Study of Greedy strategy MCQ
- 37. Concept of dynamic programming MCQ
- 38. Algorithmic Problem MCQ
- 39. Trees, Graphs, and NP-Completeness MCQ
- 40. The Software Product and Software Process MCQ
- 41. Software Design MCQ
- 42. Software Analysis and Testing MCQ
- 43. Software Maintenance & Software Project Measurement MCQ
- 44. Computer Architecture, Design, and Memory Technologies MCQ
- 45. Basic Structure of Computer MCQ
- 46. Computer Arithmetic MCQ
- 47. I/O Organization MCQ
- 48. Memory Organization MCQ
- 49. Multiprocessors MCQ
- 50. Introduction to Operating Systems MCQ

- 51. File Systems MCQ
- 52. CPU Scheduling MCQ
- 53. Memory Management MCQ
- 54. Input / Output MCQ
- 55. Operating Systems and Concurrency
- 56. Software Development and Architecture MCQ
- 57. Software architecture models MCQ
- 58. Software architecture implementation technologies MCQ
- 59. Software Architecture analysis and design MCQ
- 60. Software Architecture documentation MCQ
- 61. Introduction to Computational Intelligence MCQ
- 62. Fuzzy Systems MCQ
- 63. Genetic Algorithms MCQ
- 64. Rough Set Theory MCQ
- 65. Introduction to Swarm Intelligence, Swarm Intelligence Techniques MCQ
- 66. Neural Network History and Architectures MCQ
- 67. Autoencoder MCQ
- 68. Deep Learning MCQs
- 69. RL & Bandit Algorithms MCQs
- 70. RL Techniques MCQs
- 71. Review of traditional networks MCQ
- 72. Study of traditional routing and transport MCQ
- 73. Wireless LAN MCQ
- 74. Mobile transport layer MCQ
- 75. Big Data MCQ
- 76. Hadoop and Related Concepts MCQ
- 77. Hive, Pig, and ETL Processing MCQ

- 78. NoSQL MCQs Concepts, Variations, and MongoDB
- 79. Mining social Network Graphs MCQ
- 80. Data Warehousing MCQ
- 81. OLAP Systems MCQ
- 82. Introduction to Data& Data Mining MCQ
- 83. Supervised Learning MCQ
- 84. Clustering & Association Rule mining MCQ
- 85. Fundamentals of Agile Process MCQ
- 86. Agile Projects MCQs
- 87. Introduction to Scrum MCQs
- 88. Introduction to Extreme Programming (XP) MCQs
- 89. Agile Software Design and Development MCQs
- 90. Machine Learning Fundamentals MCQs
- 91. Neural Network MCQs
- 92. CNNs MCQ
- 93. Reinforcement Learning and Sequential Models MCQs
- 94. Machine Learning in ImageNet Competition mcq
- 95. Computer Network MCQ
- 96. Data Link Layer MCQ
- 97. MAC Sub layer MCQ
- 98. Network Layer MCQ
- 99. Transport Layer MCQ
- 100. Raster Scan Displays MCQs
- 101. 3-D Transformations MCQs
- 102. Visualization MCQ
- 103. Multimedia MCQs
- 104. Introduction to compiling & Lexical Analysis MCQs

- 105. Syntax Analysis & Syntax Directed Translation MCQs
- 106. Type Checking & Run Time Environment MCQs
- 107. Code Generation MCQs
- 108. Code Optimization MCQs
- 109. INTRODUCTION Knowledge Management MCQs
- 110. Organization and Knowledge Management MCQs
- 111. Telecommunications and Networks in Knowledge Management MCQs
- 112. Components of a Knowledge Strategy MCQs
- 113. Advanced topics and case studies in knowledge management MCQs
- 114. Conventional Software Management MCQs
- 115. Software Management Process MCQs
- 116. Software Management Disciplines MCQs
- 117. Rural Management MCQs
- 118. Human Resource Management for rural India MCQs
- 119. Management of Rural Financing MCQs
- 120. Research Methodology MCQs
- 121. Research Methodology MCQs
- 122. IoT MCQs
- 123. Sensors and Actuators MCQs
- 124. IoT MCQs: Basics, Components, Protocols, and Applications
- 125. MCQs on IoT Protocols
- 126. IoT MCQs
- 127. INTRODUCTION Block Chain Technologies MCQs
- 128. Understanding Block chain with Crypto currency MCQs
- 129. Understanding Block chain for Enterprises MCQs
- 130. Enterprise application of Block chain MCQs
- 131. Block chain application development MCQs

- 132. MCQs on Service Oriented Architecture, Web Services, and Cloud Computing
- 133. Utility Computing, Elastic Computing, Ajax MCQs
- 134. Data in the cloud MCQs
- 135. Cloud Security MCQs
- 136. Issues in cloud computinG MCQs
- 137. Introduction to modern processors MCQs
- 138. Data access optimizations MCQs
- 139. Parallel Computing MCQs
- 140. Efficient Open MP Programming MCQs
- 141. Distributed Memory parallel programming with MPI MCQs
- 142. Review of Object Oriented Concepts and Principles MCQs.
- 143. Introduction to RUP MCQs.
- 144. UML and OO Analysis MCQs
- 145. Object Oriented Design MCQs
- 146. Object Oriented Testing MCQs
- 147. CVIP Basics MCQs
- 148. Image Representation and Description MCQs
- 149. Region Analysis MCQs
- 150. Facet Model Recognition MCQs
- 151. Knowledge Based Vision MCQs
- 152. Game Design and Semiotics MCQs
- 153. Systems and Interactivity Understanding Choices and Dynamics MCQs
- 154. Game Rules Overview Concepts and Case Studies MCQs
- 155. IoT Essentials MCQs
- 156. Sensor and Actuator MCQs
- 157. IoT Networking & Technologies MCQs
- 158. MQTT, CoAP, XMPP, AMQP MCQs

- 159. IoT MCQs: Platforms, Security, and Case Studies
- 160. MCQs on Innovation and Entrepreneurship
- 161. Innovation Management MCQs
- 162. Stage Gate Method & Open Innovation MCQs
- 163. Innovation in Business: MCQs
- 164. Automata Theory MCQs
- 165. Finite Automata MCQs
- 166. Grammars MCQs
- 167. Push down Automata MCQs
- 168. Turing Machine MCQs
- 169. Database Management System (DBMS) MCQs
- 170. Relational Data models MCQs
- 171. Data Base Design MCQs
- 172. Transaction Processing Concepts MCQs
- 173. Control Techniques MCQs
- 174. DBMS Concepts & SQL Essentials MCQs
- 175. DESCRIPTIVE STATISTICS MCQs
- 176. INTRODUCTION TO BIG DATA MCQ
- 177. BIG DATA TECHNOLOGIES MCQs
- 178. PROCESSING BIG DATA MCQs
- 179. HADOOP MAPREDUCE MCQs
- 180. BIG DATA TOOLS AND TECHNIQUES MCQs
- 181. Pattern Recognition MCQs
- 182. Classification Algorithms MCQs
- 183. Pattern Recognition and Clustering MCQs
- 184. Feature Extraction & Selection Concepts and Algorithms MCQs
- 185. Pattern Recognition MCQs

- 186. Understanding Cybercrime Types and Challenges MCQs
- 187. Cybercrime MCQs
- 188. Cyber Crime and Criminal justice MCQs
- 189. Electronic Evidence MCQs
- 190. XML MCQs
- 191. System Security MCQs.
- 192. Linear Time- Invariant Systems mcqs
- 193. Control System MCQs: Basics, Feedback, and Analysis
- 194. OP-AMP applications MCQs
- 195. Radiation mcqs
- 196. NETWORKS mcqs
- 197. Satellite Services MCQs
- 198. NON-ELECTRICAL PARAMETER MEASUREMENTS mcqs
- 199. Practical Consideration and Technology in VLSI Design MCQs
- 200. Microwave Components and Circuits MCQs