1.Which cryptographic technique is used for secure key exchange over insecure channels?
a) Symmetric Key Cryptography
b) Asymmetric Key Cryptography
c) Hash Functions
d) Block Ciphers

View answer
Answer: b) Asymmetric Key Cryptography
Explanation: Asymmetric key cryptography, also known as public-key cryptography, is used for secure key exchange over insecure channels, such as the Diffie-Hellman key exchange algorithm.

2.Which algorithm is commonly used for digital signatures?
a) RSA
b) Diffie-Hellman
c) AES
d) SHA-256

View answer
Answer: a) RSA
Explanation: RSA (Rivest-Shamir-Adleman) algorithm is commonly used for digital signatures as well as encryption and key exchange.

3.Diffie-Hellman key exchange is vulnerable to which type of attack?
a) Man-in-the-Middle Attack
b) Brute Force Attack
c) Side-channel Attack

d) Birthday Attack

View answer
Answer: a) Man-in-the-Middle Attack
Explanation: Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack, where an attacker intercepts and alters communication between two parties.

4.Which asymmetric key cryptography algorithm is based on the discrete logarithm problem?
a) RSA
b) ECC (Elliptic Curve Cryptography)
c) Diffie-Hellman
d) ElGamal

View answer
Answer: c) Diffie-Hellman
Explanation: Diffie-Hellman key exchange is based on the discrete logarithm problem.

5.Which asymmetric key cryptography algorithm is particularly suitable for resource-constrained devices?
a) RSA
b) ECC (Elliptic Curve Cryptography)
c) Diffie-Hellman
d) ElGamal

View answer
Answer: b) ECC (Elliptic Curve Cryptography)
Explanation: ECC is particularly suitable for resource-constrained devices due to its shorter

key lengths compared to other algorithms like RSA.

6.Which attack aims to reveal information by observing patterns in encrypted data or using statistical analysis?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack
c) Chosen-Plaintext Attack
d) Frequency Analysis Attack

View answer
Answer: d) Frequency Analysis Attack
Explanation: Frequency analysis attack aims to reveal information by observing patterns in encrypted data or using statistical analysis.

7.Which type of attack exploits weaknesses in the implementation of cryptographic algorithms rather than breaking the algorithms themselves?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack
c) Implementation Attack
d) Side-Channel Attack

View answer
Answer: c) Implementation Attack
Explanation: Implementation attacks exploit weaknesses in the implementation of cryptographic algorithms rather than breaking the algorithms themselves.

8.Which attack involves submitting specially crafted input to a system to exploit

vulnerabilities in its cryptographic operations?
a) Chosen-Plaintext Attack
b) Chosen-Ciphertext Attack
c) Buffer Overflow Attack
d) Birthday Attack

View answer
Answer: c) Buffer Overflow Attack
Explanation: Buffer overflow attack involves submitting specially crafted input to a system to exploit vulnerabilities in its cryptographic operations.

9.Which attack aims to exploit the fact that the same plaintext is encrypted to the same ciphertext under the same key?
a) Replay Attack
b) Birthday Attack
c) Known-Plaintext Attack
d) Ciphertext-Only Attack

View answer
Answer: a) Replay Attack
Explanation: Replay attack aims to exploit the fact that the same plaintext is encrypted to the same ciphertext under the same key.

10.Which attack attempts to determine the private key by gathering pairs of corresponding plaintext and ciphertext?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack

c) Chosen-Plaintext Attack
d) Chosen-Ciphertext Attack

View answer
Answer: b) Known-Plaintext Attack
Explanation: Known-plaintext attack attempts to determine the private key by gathering pairs of corresponding plaintext and ciphertext.

11.Which asymmetric key cryptography algorithm relies on the difficulty of factoring large composite numbers?
a) RSA
b) ECC
c) ElGamal
d) Diffie-Hellman

View answer
Answer: a) RSA
Explanation: RSA relies on the difficulty of factoring large composite numbers for its security.

12.Which attack exploits information gained from observing the physical implementation of a cryptographic system, such as power consumption or electromagnetic radiation?
a) Side-Channel Attack
b) Brute Force Attack
c) Chosen-Plaintext Attack
d) Collision Attack

View answer

Answer: a) Side-Channel Attack
Explanation: Side-channel attack exploits information gained from observing the physical implementation of a cryptographic system, such as power consumption or electromagnetic radiation.

13.Which asymmetric key cryptography algorithm is based on the difficulty of solving the discrete logarithm problem in a finite field?
a) RSA
b) ECC
c) ElGamal
d) Diffie-Hellman

View answer
Answer: c) ElGamal
Explanation: ElGamal encryption algorithm is based on the difficulty of solving the discrete logarithm problem in a finite field.

14.Which type of attack involves submitting multiple queries to a cryptographic system to obtain information that can be used to compromise its security?
a) Birthday Attack
b) Chosen-Plaintext Attack
c) Chosen-Ciphertext Attack
d) Ciphertext-Only Attack

View answer
Answer: c) Chosen-Ciphertext Attack
Explanation: Chosen-ciphertext attack involves submitting multiple queries to a

cryptographic system to obtain information that can be used to compromise its security.

15.Which attack aims to find two different inputs that produce the same hash value?
a) Brute Force Attack
b) Collision Attack
c) Rainbow Table Attack
d) Dictionary Attack

View answer
Answer: b) Collision Attack
Explanation: Collision attack aims to find two different inputs that produce the same hash value.

16.Which asymmetric key cryptography algorithm is widely used for secure key exchange?
a) RSA
b) Diffie-Hellman
c) ElGamal
d) ECC

View answer
Answer: b) Diffie-Hellman
Explanation: Diffie-Hellman algorithm is widely used for secure key exchange.

17.Which attack involves intercepting and altering communication between two parties without their knowledge?
a) Replay Attack
b) Man-in-the-Middle Attack

c) Chosen-Plaintext Attack
d) Known-Plaintext Attack

View answer
Answer: b) Man-in-the-Middle Attack
Explanation: Man-in-the-middle attack involves intercepting and altering communication between two parties without their knowledge.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Symmetric Key Cryptography MCQ
5. Authentication & Integrity MCQ
6. E-mail, IP and Web Security MCQ
7. Introduction to Energy Science MCQ
8. Ecosystems MCQ
9. Biodiversity and its conservation MCQ
10. Environmental Pollution mcq
11. Social Issues and the Environment MCQ
12. Field work mcq
13. Discrete Structure MCQ
14. Set Theory, Relation, and Function MCQ
15. Propositional Logic and Finite State Machines MCQ
16. Graph Theory and Combinatorics MCQ
17. Relational algebra,Functions and graph theory MCQ
18. Data Structure MCQ

19. Stacks MCQ
20. TREE MCQ
21. Graphs MCQ
22. Sorting MCQ
23. Digital Systems MCQ
24. Combinational Logic MCQ
25. Sequential logic MCQ
26. Analog/Digital Conversion, Logic Gates, Multivibrators, and IC 555 MCQ
27. Introduction to Digital Communication MCQ
28. Introduction to Object Oriented Thinking & Object Oriented Programming MCQ
29. Encapsulation and Data Abstraction MCQ
30. MCQ
31. Relationships – Inheritance MCQ
32. Polymorphism MCQ
33. Library Management System MCQ
34. Numerical Methods MCQ
35. Transform Calculus MCQ
36. Concept of Probability MCQ
37. Algorithms, Designing MCQ
38. Study of Greedy strategy MCQ
39. Concept of dynamic programming MCQ
40. Algorithmic Problem MCQ
41. Trees, Graphs, and NP-Completeness MCQ
42. The Software Product and Software Process MCQ
43. Software Design MCQ
44. Software Analysis and Testing MCQ
45. Software Maintenance & Software Project Measurement MCQ

46. Computer Architecture, Design, and Memory Technologies MCQ
47. Basic Structure of Computer MCQ
48. Computer Arithmetic MCQ
49. I/O Organization MCQ
50. Memory Organization MCQ
51. Multiprocessors MCQ
52. Introduction to Operating Systems MCQ
53. File Systems MCQ
54. CPU Scheduling MCQ
55. Memory Management MCQ
56. Input / Output MCQ
57. Operating Systems and Concurrency
58. Software Development and Architecture MCQ
59. Software architecture models MCQ
60. Software architecture implementation technologies MCQ
61. Software Architecture analysis and design MCQ
62. Software Architecture documentation MCQ
63. Introduction to Computational Intelligence MCQ
64. Fuzzy Systems MCQ
65. Genetic Algorithms MCQ
66. Rough Set Theory MCQ
67. Introduction to Swarm Intelligence, Swarm Intelligence Techniques MCQ
68. Neural Network History and Architectures MCQ
69. Autoencoder MCQ
70. Deep Learning MCQs
71. RL & Bandit Algorithms MCQs
72. RL Techniques MCQs

73. Review of traditional networks MCQ
74. Study of traditional routing and transport MCQ
75. Wireless LAN MCQ
76. Mobile transport layer MCQ
77. Big Data MCQ
78. Hadoop and Related Concepts MCQ
79. Hive, Pig, and ETL Processing MCQ
80. NoSQL MCQs Concepts, Variations, and MongoDB
81. Mining social Network Graphs MCQ
82. Mathematical Background for Cryptography MCQ
83. Cryptography MCQ
84. Cryptographic MCQs
85. Information Security MCQ
86. Cryptography and Information Security Tools MCQ
87. Data Warehousing MCQ
88. OLAP Systems MCQ
89. Introduction to Data& Data Mining MCQ
90. Supervised Learning MCQ
91. Clustering & Association Rule mining MCQ
92. Fundamentals of Agile Process MCQ
93. Agile Projects MCQs
94. Introduction to Scrum MCQs
95. Introduction to Extreme Programming (XP) MCQs
96. Agile Software Design and Development MCQs
97. Machine Learning Fundamentals MCQs
98. Neural Network MCQs
99. CNNs MCQ

100. Reinforcement Learning and Sequential Models MCQs
101. Machine Learning in ImageNet Competition mcq
102. Computer Network MCQ
103. Data Link Layer MCQ
104. MAC Sub layer MCQ
105. Network Layer MCQ
106. Transport Layer MCQ
107. Raster Scan Displays MCQs
108. 3-D Transformations MCQs
109. Visualization MCQ
110. Multimedia MCQs
111. Introduction to compiling & Lexical Analysis MCQs
112. Syntax Analysis &Syntax Directed Translation MCQs
113. Type Checking & Run Time Environment MCQs
114. Code Generation MCQs
115. Code Optimization MCQs
116. INTRODUCTION Knowledge Management MCQs
117. Organization and Knowledge Management MCQs
118. Telecommunications and Networks in Knowledge Management MCQs
119. Components of a Knowledge Strategy MCQs
120. Advanced topics and case studies in knowledge management MCQs
121. Conventional Software Management MCQs
122. Software Management Process MCQs
123. Software Management Disciplines MCQs
124. Rural Management MCQs
125. Human Resource Management for rural India MCQs
126. Management of Rural Financing MCQs

127. Research Methodology MCQs
128. Research Methodology MCQs
129. IoT MCQs
130. Sensors and Actuators MCQs
131. IoT MCQs: Basics, Components, Protocols, and Applications
132. MCQs on IoT Protocols
133. IoT MCQs
134. INTRODUCTION Block Chain Technologies MCQs
135. Understanding Block chain with Crypto currency MCQs
136. Understanding Block chain for Enterprises MCQs
137. Enterprise application of Block chain MCQs
138. Block chain application development MCQs
139. MCQs on Service Oriented Architecture, Web Services, and Cloud Computing
140. Utility Computing, Elastic Computing, Ajax MCQs
141. Data in the cloud MCQs
142. Cloud Security MCQs
143. Issues in cloud computinG MCQs
144. Introduction to modern processors MCQs
145. Data access optimizations MCQs
146. Parallel Computing MCQs
147. Efficient Open MP Programming MCQs
148. Distributed Memory parallel programming with MPI MCQs
149. Review of Object Oriented Concepts and Principles MCQs.
150. Introduction to RUP MCQs.
151. UML and OO Analysis MCQs
152. Object Oriented Design MCQs
153. Object Oriented Testing MCQs

154. CVIP Basics MCQs
155. Image Representation and Description MCQs
156. Region Analysis MCQs
157. Facet Model Recognition MCQs
158. Knowledge Based Vision MCQs
159. Game Design and Semiotics MCQs
160. Systems and Interactivity Understanding Choices and Dynamics MCQs
161. Game Rules Overview Concepts and Case Studies MCQs
162. IoT Essentials MCQs
163. Sensor and Actuator MCQs
164. IoT Networking & Technologies MCQs
165. MQTT, CoAP, XMPP, AMQP MCQs
166. IoT MCQs: Platforms, Security, and Case Studies
167. MCQs on Innovation and Entrepreneurship
168. Innovation Management MCQs
169. Stage Gate Method & Open Innovation MCQs
170. Innovation in Business: MCQs
171. Automata Theory MCQs
172. Finite Automata MCQs
173. Grammars MCQs
174. Push down Automata MCQs
175. Turing Machine MCQs
176. Database Management System (DBMS) MCQs
177. Relational Data models MCQs
178. Data Base Design MCQs
179. Transaction Processing Concepts MCQs
180. Control Techniques MCQs

181. DBMS Concepts & SQL Essentials MCQs
182. DESCRIPTIVE STATISTICS MCQs
183. INTRODUCTION TO BIG DATA MCQ
184. BIG DATA TECHNOLOGIES MCQs
185. PROCESSING BIG DATA MCQs
186. HADOOP MAPREDUCE MCQs
187. BIG DATA TOOLS AND TECHNIQUES MCQs
188. Pattern Recognition MCQs
189. Classification Algorithms MCQs
190. Pattern Recognition and Clustering MCQs
191. Feature Extraction & Selection Concepts and Algorithms MCQs
192. Pattern Recognition MCQs
193. Understanding Cybercrime Types and Challenges MCQs
194. Cybercrime MCQs
195. Cyber Crime and Criminal justice MCQs
196. Electronic Evidence MCQs