1.Which classical cryptographic technique involves replacing each plaintext character with another character?
a) Substitution
b) Transposition
c) Symmetric key cryptography
d) Asymmetric key cryptography

View answer
Answer: a) Substitution
Explanation: Substitution involves replacing each plaintext character with another character according to a predetermined key or rule.

2.What is the primary goal of transposition in classical cryptography?
a) Replacing characters with others
b) Rearranging the order of characters
c) Encrypting data with multiple keys
d) Increasing the key size

View answer
Answer: b) Rearranging the order of characters
Explanation: Transposition involves rearranging the order of characters in the plaintext to create the ciphertext.

3.Which classical cryptographic attack involves analyzing the frequency of characters to decrypt a message?
a) Linear cryptanalysis
b) Differential cryptanalysis

c) Frequency analysis
d) Brute force attack

View answer
Answer: c) Frequency analysis
Explanation: Frequency analysis is a classical cryptanalysis technique where the frequency of characters in the ciphertext is analyzed to identify patterns and decrypt the message.

4.Which symmetric key encryption algorithm was widely used in the past but is now considered insecure due to its short key length?
a) DES
b) AES
c) 3DES
d) RSA

View answer
Answer: a) DES
Explanation: DES (Data Encryption Standard) was widely used in the past but is now considered insecure due to its short key length.

5.Which of the following is NOT a mode of operation in symmetric key cryptography?
a) ECB
b) CBC
c) RSA
d) CTR

View answer

Answer: c) RSA
Explanation: RSA is an asymmetric key algorithm, not a mode of operation in symmetric key cryptography.

6.In which mode of operation does each block of plaintext get XORed with the previous block of ciphertext before encryption?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: b) CBC
Explanation: In CBC (Cipher Block Chaining) mode, each block of plaintext is XORed with the previous block of ciphertext before encryption.

7.Which cryptanalysis technique relies on analyzing the correlation between the bits of plaintext, ciphertext, and the encryption key?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: b) Differential cryptanalysis
Explanation: Differential cryptanalysis relies on analyzing the correlation between the bits of plaintext, ciphertext, and the encryption key to break the cipher.

8.Which symmetric key encryption algorithm uses a Feistel network structure?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: c) 3DES
Explanation: 3DES (Triple Data Encryption Standard) uses a Feistel network structure to encrypt data.

9.Which mode of operation is vulnerable to a padding oracle attack?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: b) CBC
Explanation: CBC (Cipher Block Chaining) mode is vulnerable to a padding oracle attack.

10.Which symmetric key encryption algorithm is known for its flexibility in supporting key sizes and block sizes?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: d) Blowfish
Explanation: Blowfish is known for its flexibility in supporting key sizes and block sizes.

11.What is the primary disadvantage of using the ECB mode of operation?
a) It requires a large initialization vector (IV).
b) It does not provide confidentiality for identical plaintext blocks.
c) It is vulnerable to padding oracle attacks.
d) It is slower compared to other modes.

View answer
Answer: b) It does not provide confidentiality for identical plaintext blocks.
Explanation: ECB (Electronic Codebook) mode does not provide confidentiality for identical plaintext blocks as identical blocks of plaintext are encrypted into identical blocks of ciphertext.

12.Which cryptanalysis technique focuses on exploiting the linearity of a cipher?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: a) Linear cryptanalysis
Explanation: Linear cryptanalysis focuses on exploiting the linearity of a cipher to break it.

13.In which mode of operation does each plaintext block get encrypted separately and

independently?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: a) ECB
Explanation: ECB (Electronic Codebook) mode encrypts each plaintext block separately and independently.

14.Which symmetric key encryption algorithm is commonly used for securing electronic communication over the Internet?
a) AES
b) DES
c) 3DES
d) Blowfish

View answer
Answer: a) AES
Explanation: AES (Advanced Encryption Standard) is commonly used for securing electronic communication over the Internet.

15.Which mode of operation is primarily used for full disk encryption and random access data?
a) ECB
b) CBC

c) CTR
d) OFB

View answer
Answer: c) CTR
Explanation: CTR (Counter) mode is primarily used for full disk encryption and random access data.

16.Which cryptanalysis technique involves observing the changes in the ciphertext when the plaintext is slightly altered?
a) Linear cryptanalysis
b) Differential cryptanalysis
c) Frequency analysis
d) Brute force attack

View answer
Answer: b) Differential cryptanalysis
Explanation: Differential cryptanalysis involves observing the changes in the ciphertext when the plaintext is slightly altered to break the cipher.

17.Which symmetric key encryption algorithm is also known as Rijndael?
a) DES
b) AES
c) 3DES
d) Blowfish

View answer

Answer: b) AES
Explanation: AES (Advanced Encryption Standard) is also known as Rijndael.

18.Which mode of operation XORs the plaintext with a random value generated for each block before encryption?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: d) OFB
Explanation: OFB (Output Feedback) mode XORs the plaintext with a random value generated for each block before encryption.

19.Which symmetric key encryption algorithm is a variant of DES that uses three rounds of encryption for increased security?
a) DES
b) AES
c) 3DES
d) Blowfish

View answer
Answer: c) 3DES
Explanation: 3DES (Triple Data Encryption Standard) is a variant of DES that uses three rounds of encryption for increased security.

20.Which mode of operation is recommended for its parallelizability and resistance to timing attacks?
a) ECB
b) CBC
c) CTR
d) OFB

View answer
Answer: c) CTR
Explanation: CTR (Counter) mode is recommended for its parallelizability and resistance to timing attacks.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Asymmetric 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