1. What branch of mathematics forms the foundation of modern cryptography?

a) Calculus
b) Geometry
c) Abstract Algebra
d) Trigonometry

Answer: c) Abstract Algebra

Explanation: Abstract Algebra, particularly concepts like groups, rings, and fields, provides the mathematical framework used in cryptographic algorithms.

2. Which mathematical concept is used to encrypt data in the RSA algorithm?

a) Prime factorization
b) Differential equations
c) Matrix multiplication
d) Integration

Answer: a) Prime factorization

Explanation: RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors.

3. What is the primary purpose of the Extended Euclidean Algorithm in cryptography?

a) Generating prime numbers
b) Finding modular inverses

c) Generating random keys
d) Performing frequency analysis

Answer: b) Finding modular inverses

Explanation: The Extended Euclidean Algorithm is used to find the modular inverse of a number, which is crucial in many cryptographic operations, such as RSA encryption and decryption.

4. Which theorem states that if p is a prime number and a is an integer not divisible by p, then (a^{p-1}) is congruent to 1 modulo p?

a) Euler's Theorem
b) Fermat's Little Theorem
c) Wilson's Theorem
d) Lagrange's Theorem

Answer: b) Fermat's Little Theorem

Explanation: Fermat's Little Theorem is a fundamental theorem in number theory that has significant applications in cryptography.

5. What is the purpose of the Euler Phi-Function in cryptography?

a) Generating prime numbers
b) Calculating modular inverses
c) Calculating the number of relatively prime integers
d) Generating random keys

Answer: c) Calculating the number of relatively prime integers

Explanation: The Euler Phi-Function ((\phi(n))) calculates the number of positive integers less than n that are relatively prime to n, which is essential in cryptographic algorithms like RSA.

6. Which classical cryptosystem uses a 5×5 grid of letters for encryption?

a) Caesar Cipher
b) Playfair Cipher
c) Vigenère Cipher
d) Atbash Cipher

Answer: b) Playfair Cipher

Explanation: The Playfair Cipher encrypts pairs of letters using a 5×5 grid of letters, known as a Playfair Square.

7. What technique is commonly used to break the substitution cipher by analyzing letter frequencies?

a) Differential cryptanalysis
b) Frequency analysis
c) Linear cryptanalysis
d) Brute-force attack

Answer: b) Frequency analysis

Explanation: Frequency analysis involves analyzing the frequency of letters or symbols in a ciphertext to deduce information about the plaintext.

8. Which of the following is NOT a block cipher?

a) AES
b) DES
c) RSA
d) Blowfish

Answer: c) RSA

Explanation: RSA is a public-key encryption algorithm, whereas AES, DES, and Blowfish are block ciphers.

9. Which mode of operation is commonly used for encrypting large files with block ciphers?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: b) CBC (Cipher Block Chaining)

Explanation: CBC mode is commonly used for encrypting large files because it introduces diffusion and prevents patterns in the plaintext from being apparent in the ciphertext.

10. Which encryption standard is based on the Feistel cipher structure?

a) AES
b) DES
c) RSA
d) ElGamal

Answer: b) DES

Explanation: DES (Data Encryption Standard) is based on the Feistel cipher structure, which involves multiple rounds of substitution and permutation.

11. Which cipher operates on individual characters or bits of plaintext one at a time?

a) Block Cipher
b) Stream Cipher
c) Public Key Cipher
d) Transposition Cipher

Answer: b) Stream Cipher

Explanation: Stream ciphers encrypt plaintext one bit or character at a time, typically using a keystream generator.

12. What is the key length of Triple DES (3DES)?

a) 56 bits
b) 112 bits
c) 128 bits
d) 168 bits

Answer: b) 112 bits

Explanation: Triple DES (3DES) has a key length of 112 bits, derived from its three stages of DES encryption.

13. Which mode of operation XORs the plaintext with the output of a pseudorandom keystream generator?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: d) OFB (Output Feedback)

Explanation: OFB mode XORs the plaintext with the output of a pseudorandom keystream generator, which is then fed back to generate subsequent keystreams.

14. In which classical cipher does each letter in the plaintext get replaced by a letter some fixed number of positions down the alphabet?

a) Caesar Cipher
b) Playfair Cipher
c) Rail Fence Cipher
d) Affine Cipher

Answer: a) Caesar Cipher

Explanation: The Caesar Cipher is a substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down or up the alphabet.

15. Which type of cryptanalysis involves using known plaintext and corresponding ciphertext pairs to deduce the key?

a) Differential cryptanalysis
b) Frequency analysis
c) Known-plaintext attack
d) Chosen-plaintext attack

Answer: c) Known-plaintext attack

Explanation: Known-plaintext attacks exploit the knowledge of plaintext-ciphertext pairs to deduce information about the encryption key.

16. Which cryptographic principle states that the security of the system should not depend on keeping the algorithm secret, but rather on keeping the key secret?

a) Kerckhoffs’s Principle
b) Diffie-Hellman Principle
c) Shannon’s Principle
d) Turing’s Principle

Answer: a) Kerckhoffs’s Principle

Explanation: Kerckhoffs’s Principle states that the security of a cryptographic system should rely on the secrecy of the key rather than the secrecy of the algorithm itself.

17. Which cipher mode is vulnerable to a watermarking attack?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: a) ECB (Electronic Codebook)

Explanation: ECB mode encrypts identical plaintext blocks into identical ciphertext blocks, making it vulnerable to a watermarking attack where patterns in the plaintext can be discerned from the ciphertext.

18. Which mode of operation is known for its parallelizability and efficiency in hardware implementations?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: c) CTR (Counter)

Explanation: CTR mode turns a block cipher into a stream cipher, allowing for parallel encryption and decryption, making it efficient for hardware implementations.

19. What type of cipher uses a key to perform a series of transformations on the plaintext?

a) Symmetric Cipher
b) Asymmetric Cipher
c) Hash Function
d) Steganography

Answer: a) Symmetric Cipher

Explanation: Symmetric ciphers use the same key for both encryption and decryption to perform a series of transformations on the plaintext.

20. Which cryptographic technique ensures data integrity by generating a fixed-size hash based on the input data?

a) Encryption
b) Digital Signature
c) Key Exchange
d) Hash Function

Answer: d) Hash Function

Explanation: Hash functions generate fixed-size hash values based on the input data, which can be used to verify the integrity of the data without revealing the original content.

Related posts:

1. Cryptography MCQ
2. Cryptographic MCQs
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. Introduction to Information Security
191. Web Development Essentials MCQs
192. C Programming Essentials Structures, Preprocessor, and Unions MCQs

193. The Shell Basic Commands, Shell Programming MCQs
194. Environmental Pollution mcqs
195. Modulation Techniques mcqs
196. Feedback Amplifiers and Oscillators MCQs
197. Frequency Analysis of Discrete Time Signals mcqs
198. Data Communication mcqs
199. Satellite Communication & Polarization MCQs
200. Input Output and Peripheral Devices mcqs