



1. Which of the following is not a diagram studied in Requirement Analysis?

- A. Use Cases
- B. Entity Relationship Diagram
- C. State Transition Diagram
- D. Activity Diagram

2. How many feasibility studies is conducted in Requirement Analysis ?

- A. Two
- B. Three
- C. Four
- D. None of the mentionedA.

3. Which of the following is not a direct measure of SE process?

- A. Efficiency
- B. Cost
- C. Effort Applied
- D. All of the mentioned

4. Requirements Analysis is an Iterative Process.

- A. True
- B. False

5. Prototyping in software process may involve \_\_\_\_\_

- A. throw - away prototyping
- B. evolutionary
- C. Both a and b options
- D. None of these

6. Which of the following is the task of project indicators:

- A. help in assessment of status of on going project
- B. Track potential risk
- C. help in assessment of status of on-going project & track potential risk
- D. none of the mentioned

7. Which of the following does not affect the software quality and organizational performance?

- A. Market
- B. Product
- C. Technology
- D. People

8. Which of the following is an indirect measure of product?

- A. Quality
- B. Complexity
- C. Reliability
- D. All of the Mentioned

9. Which of the following is not a direct measure of SE process?

- A. Efficiency
- B. Cost
- C. Effort Applied
- D. All of the mentioned



10. Which of the following is an indirect measure of product?

- A. Quality
- B. Complexity
- C. Reliability
- D. All of the Mentioned

11. In size oriented metrics, metrics are developed based on the \_\_\_\_\_

- A. number of Functions
- B. number of user inputs
- C. number of lines of code
- D. amount of memory usage

12. Which of the following is not an information domain required for determining function point in FPA ?

- A. Number of user Input
- B. Number of user Inquiries
- C. Number of external Interfaces
- D. Number of errors

13. Usability can be measured in terms of:

- A. Intellectual skill to learn the system
- B. Time required to become moderately efficient in system usage
- C. Net increase in productivity
- D. All of the mentioned



14. A graphical technique for finding if changes and variation in metrics data are meaningful is known as

- A. DRE (Defect Removal Efficiency)
- B. Function points analysis
- C. Control Chart
- D. All of the mentioned

15. Defects removal efficiency (DRE) depends on:

- A. E – errors found before software delivery
- B. D – defects found after delivery to user
- C. Both E and D
- D. Varies with project

16. Which of the following is not included in failure costs?

- A. rework
- B. repair
- C. failure mode analysis
- D. none of the mentioned

17. Which requirements are the foundation from which quality is measured?

- A. Hardware
- B. Software
- C. Programmers
- D. None of the mentioned

18. Which of the following is not a SQA plan for a project?

- A. evaluations to be performed
- B. amount of technical work
- C. audits and reviews to be performed
- D. documents to be produced by the SQA group

19. Degree to which design specifications are followed in manufacturing the product is called





- A. Quality Control
- B. Quality of conformance
- C. Quality Assurance
- D. None of the mentioned

20. Which of the following is not included in External failure costs?

- A. testing
- B. help line support
- C. warranty work
- D. complaint resolution

21. Which of the following is not an appraisal cost in SQA?

- A. inter-process inspection
- B. maintenance
- C. quality planning
- D. testing

22. The primary objective of formal technical reviews is to find \_\_\_\_\_ during the process so that they do not become defects after release of the software.

- A. errors
- B. equivalent faults
- C. failure cause
- D. none of the mentioned

23. What is not included in prevention costs?

- A. Quality planning
- B. Formal technical reviews
- C. Test equipment
- D. Equipment calibration and maintenance

24. Software quality assurance consists of the auditing and reporting functions of management.

- A. True
- B. False



25. Who identifies, documents, and verifies that corrections have been made to the software?

- A. Project manager
- B. Project team
- C. SQA group
- D. All of the mentioned

26. Which of the following is not a metric for design model?

- A. Interface design metrics
- B. Component-level metrics
- C. Architectural metrics
- D. Complexity metrics

27. Statement and branch coverage metrics are part of

- A. Analysis Model
- B. Testing
- C. Design Model
- D. Source Code

28. Function Points in software engineering was first proposed by

- A. Booch
- B. Boehm
- C. Albrecht
- D. Jacobson

29. How many Information Domain Values are used for Function Point Computation?

- A. three
- B. four
- C. five
- D. six

30. SMI stands for

- A. Software Mature Indicator
- B. Software Maturity Index
- C. Software Mature Index

D. Software Maturity Indicator

31.  $SMI = [M_t - (F_a + F_c + F_d)]/M_t$ . Here  $M_t$  is the number of modules

- A. in the current release
- B. in the current release that have been changed
- C. from the preceding release that were deleted in the current release
- D. none of the mentioned

32. The amount of time that the software is available for use is known as

- A. Reliability
- B. Usability
- C. Efficiency
- D. Functionality

33. Usability in metric analysis is defined as the degree to which the software

- A. stated needs
- B. is easy to use
- C. makes optimal use of system resources
- D. none of the mentioned

34. \_\_\_\_\_ model consists of the particular types of services that you can access on a cloud computing platform.

- A. Service
- B. Deployment
- C. Application
- D. None of the mentioned

35. Point out the correct statement.



- A. The use of the word “cloud” makes reference to the two essential concepts
- B. Cloud computing abstracts systems by pooling and sharing resources
- C. cloud computing is nothing more than the Internet
- D. All of the mentioned

36. \_\_\_\_\_ refers to the location and management of the cloud’s infrastructure.

- A. Service
- B. Deployment
- C. Application
- D. None of the mentioned

37. Which of the following is the deployment model?

- A. public
- B. private
- C. hybrid
- D. all of the mentioned

38. Point out the wrong statement.

- A. Cloud Computing has two distinct sets of models
- B. Amazon has built a worldwide network of datacenters to service its search engine
- C. Azure enables .NET Framework applications to run over the Internet
- D. None of the mentioned

39. Which of the following is best known service model?

- A. SaaS
- B. IaaS
- C. PaaS
- D. All of the mentioned





40. The \_\_\_\_\_ model originally did not require a cloud to use virtualization to pool resources.

- A. NEFT
- B. NIST
- C. NIT
- D. All of the mentioned

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
D	B	A	A	C	C	A	D	A	D	C	D	D	C	C	D	B	B	B	a
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
C	A	D	A	C	D	B	C	C	B	A	D	B	A	B	B	D	B	D	B



41. A distributed database has which of the following advantages over a centralized database?

- A. Software cost
- B. Software complexity
- C. Slow Response
- D. Modular growth

42. An autonomous homogenous environment is which of the following?

- A. The same DBMS is at each node and each DBMS works independently.
- B. The same DBMS is at each node and a central DBMS coordinates database access.
- C. A different DBMS is at each node and each DBMS works independently.
- D. A different DBMS is at each node and a central DBMS coordinates database access.

43. A transaction manager is which of the following?

- A. Maintains a log of transactions
- B. Maintains before and after database images
- C. Maintains appropriate concurrency control
- D. All of the above.

44. Let us suppose that in a distributed database, during a transaction T1, one of the sites, say S1, is failed. When recovers, the site S1 has to check its log file (log based recovery) to decide the next move on the transaction T1. If the log contains a <commit T> record, what the site S1 has to do?

- A. Need not do anything
- B. Perform Undo
- C. Perform Redo
- D. Abort the transaction

45. Global Wait-for graph is used for \_\_\_\_\_ in Distributed database.

- A. Handling concurrency control
- B. Handling failures



- C. Handling deadlock
- D. None of the above

46. In Distributed database, \_\_\_\_\_ are the transactions for which a <ready T> log is found in the log file, but neither a <commit T> log nor an <abort T> log is found.

- A. In-doubt transactions
- B. Serialized transactions
- C. Cascadeless transactions
- D. Distributed transactions

47. While using commit protocols for handling atomicity issues, the distributed database system may enter into a situation called Blocking problem. Which of the following commit protocols can avoid Blocking problem?

- A. Two-phase commit protocol
- B. Three-phase commit protocol
- C. Both of the above
- D. None of the above

48. Which of the following concurrency control protocol is suitable for an application where frequency of read operation is much greater than that of write operation?

- A. Majority protocol
- B. Quorum-consensus protocol
- C. Biased protocol
- D. Single lock protocol

49. Which of the following parallel database architectures is/are mainly used by distributed database system?

- A. Shared Memory
- B. Shared Disk
- C. Shared Nothing
- D. Hierarchical

**50. Which of the following is not a promise of distributed database?**

- A. Network Transparency
- B. Replication Transparency
- C. Fragmentation Transparency
- D. None of the above

**51. A data warehouse is which of the following?**

- A. Can be updated by end users.
- B. Contains numerous naming conventions and formats.
- C. Organized around important subject areas.
- D. Contains only current data.

**52. Data transformation includes which of the following?**

- A. A process to change data from a detailed level to a summary level
- B. A process to change data from a summary level to a detailed level
- C. Joining data from one source into various sources of data
- D. Separating data from one source into various sources of data

**53. A multifield transformation does which of the following?**

- A. Converts data from one field into multiple fields
- B. Converts data from multiple fields into one field
- C. Converts data from multiple fields into multiple fields
- D. All of the above

**54. Which of the following features usually applies to data in a data warehouse?**

- A. Data are often deleted
- B. Most applications consist of transactions
- C. Data are rarely deleted
- D. Relatively few records are processed by applications

**55. Which of the following statement is true?**

- A. The data warehouse consists of data marts and operational data



- B. The data warehouse is used as a source for the operational data
- C. The operational data are used as a source for the data warehouse
- D. All of the above

**56. The following is true of three-tier data warehouses:**

- A. Once created, the data marts will keep on being updated from the data warehouse at periodic times
- B. Once created; the data marts will directly receive their new data from the operational databases
- C. The data marts are different groups of tables in the data warehouse
- D. A data mart becomes a data warehouse when it reaches a critical size

**57.The following technology is not well-suited for data mining:**

- A.Expert system technology
- B.Data visualization
- C.Technology limited to specific data types such as numeric data types
- D.Parallel architecture

**58. What is true of the multidimensional model?**

- A.It typically requires less disk storage
- B.It typically requires more disk storage
- C. Typical business queries requiring aggregate functions take more time
- D. Increasing the size of a dimension is difficult

**59. The extract process is which of the following?**





- A. Capturing all of the data contained in various operational systems
- B. Capturing a subset of the data contained in various operational systems
- C. Capturing all of the data contained in various decision support systems
- D. Capturing a subset of the data contained in various decision support systems

**60. A data warehouse is which of the following?**

- A. Can be updated by end users.
- B. Contains numerous naming conventions and formats.
- C. Organized around important subject areas.
- D. Contains only current data.





61.All sites in a distributed database commit at exactly the same instant. TRUE/FALSE

- A. TRUE
- B. FALSE

62.The real use of the Two-phase commit protocol is \_\_\_\_\_

- A. Deadlock will not occur
- B. Concurrency control can be avoided
- C. Atomicity, i.e, all-or-nothing commits at all sites
- D. None of the above

63. Read one, write all available protocol is used to increase \_\_\_\_\_ in a distributed database system.

- A. Availability
- B. Robustness
- C. Both Availability and Robustness
- D. Neither Availability nor Robustness

64. What is the size of the key in the SDES algorithm?

- A. 24 bits
- B. 16 bits
- C. 20 bits
- D. 10 bits

65. Assume input 10-bit key, K: 101000010 for the SDES algorithm. What is K1?

- A. 10100100
- B. 01011011
- C. 01101000
- D. 10100111

66.Assume input 10-bit key, K: 101000010 for the SDES algorithm. What is K2?

- A. 10100111
- B. 01000011



- C. 00100100
- D. 01011010

67. The Plaintext for the Ciphertext 00100010, given that the key is 111111111 is

- A. 01100111
- B. 00001010
- C. 01001000
- D. 01001100

68. Assume input 10-bit key, K: 0010010111 for the SDES algorithm. What is K1?

- A. 00101111
- B. 01011011
- C. 01101000
- D. 10100111

69. The Plaintext for the Ciphertext 00001111, given that the key is 1111111111 is

- A. 01100111
- B. 00001010
- C. 11111111
- D. 01101101

70. The Plaintext for the Ciphertext 11110000, given that the key is 0000000000 is

- A. 01100111
- B. 00000000
- C. 01001000
- D. 01101100

71. The process of transforming plain text into unreadable text.

- A. Decryption
- B. Encryption
- C. Network Security
- D. Information Hiding

72. An algorithm used in encryption is referred to as cipher.

- A. True



B. False

73. A process of making the encrypted text readable again.

- A. Decryption
- B. Encryption
- C. Network Security
- D. Information Hiding

74. A cipher in which the order is not preserved.

- A. Polyalphabetic substitution based
- B. Transposition-based
- C. Substitution based
- D. Public key based

75. Study of creating a d using encryption and decryption techniques.

- A. Cipher
- B. Cryptography
- C. Encryption
- D. Decryption

76. These ciphers replace a character or characters with a different character or characters, based on some key.

- A. Polyalphabetic substitution based
- B. Transposition-based
- C. Substitution based
- D. Mono alphabetic substitution based

77. Encryption is the study of creating and using decryption techniques.

- A. True
- B. False

78. An encryption technique with 2 keys is \_\_\_\_\_



- A. Monoalphabetic Cipher
- B. Cryptography
- C. Private key cryptography
- D. Public key cryptography

79. A type of cipher that uses multiple alphabetic strings.

- A. Substitution based
- B. Transposition-based
- C. Polyalphabetic substitution based
- D. Mono alphabetic substitution based

80. Encryption is the study of creating and using decryption techniques.

- A. True
- B. False

41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
D	A	D	B	C	A	B	C	C	D	C	A	D	C	C	A	C	B	B	C
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
B	C	C	D	A	B	D	A	D	B	B	A	A	B	B	D	B	D	C	B



**81. These ciphers replace a character or characters with a different character or characters, based on some key.**

- A. Polyalphabetic substitution based
- B. Transposition-based
- C. Substitution based
- D. Mono alphabetic substitution based

**82. The keys used in cryptography are**

- A. secret key
- B. private key
- C. public key
- D. All of them

**83.In symmetric-key cryptography, the key locks and unlocks the box is**

- A. same
- B. shared
- C. private
- D. public

**84.Symmetric-key cryptography started thousands of years ago when people needed to exchange**

- A. Files
- B. Packets
- C. Secrets
- D. Transmission

**85. Cryptography, a word with Greek origins, means**

- A. Corrupting Data
- B. Secret Writing
- C. Open Writing



D. Closed Writing

**86. A transposition cipher reorders (permutes) symbols in a**

- A. block of packets
- B. block of slots
- C. block of signals
- D. block of symbols

**87. The Advanced Encryption Standard (AES) was designed**

- A. National Institute of Standards and Technology
- B. IBM
- C. HP
- D. Intel

**88. The Cryptography can provide**

- A. entity authentication
- B. nonrepudiation of messages
- C. confidentiality
- D. All of them

**89. The Data Encryption Standard (DES) was designed by**

- A. Microsoft
- B. Apple
- C. IBM
- D. None

**90. The process of transforming plain text to unreadable text.**

- A. Decryption
- B. Encryption
- C. Network Security
- D. Information Hiding

**91. \_\_\_\_\_ model attempts to categorize a cloud network based on four dimensional factors.**

- A. Cloud Square
- B. Cloud Service



- C. Cloud Cube
- D. All of the mentioned

92. How many types of dimensions exists in Cloud Cube Model?

- A. 1
- B. 2
- C. 3
- D. 4

93. Which of the following dimension is related to organization's boundaries?

- A. Physical location of data
- B. Ownership
- C. Security boundary
- D. All of the mentioned

94. Which of the following is related to the service provided by Cloud?

- A. Sourcing
- B. Ownership
- C. Reliability
- D. AaaS

95. Which of the following was one of the top 5 cloud applications in 2010?

- A. Cloud backup
- B. Web applications
- C. Business applications
- D. All of the mentioned

96. Point out the correct statement.

- A. Google's cloud includes perhaps some 10 data centers worldwide
- B. Flipkart.com's infrastructure was built to support elastic demand so the system could accommodate peak traffic
- C. Data centers have been sited to optimize the overall system latency
- D. All of the mentioned



97. Which of the following benefit is related to creates resources that are pooled together in a system that supports multi-tenant usage?

- A. On-demand self-service
- B. Broad network access
- C. Resource pooling
- D. All of the mentioned

98. The \_\_\_\_\_ is something that you can obtain under contract from your vendor.

- A. PoS
- B. QoS
- C. SoS
- D. All of the mentioned

99. Point out the wrong statement.

- A. Internet consumes roughly 1 percent of the world's total power
- B. The cost advantages of cloud computing have enabled new software vendors to create productivity applications
- C. A client can provision computer resources without the need for interaction with cloud service provider personnel
- D. None of the mentioned

100. All cloud computing applications suffer from the inherent \_\_\_\_\_ that is intrinsic in their WAN connectivity.

- A. propagation
- B. latency
- C. noise
- D. all of the mentioned

101. Cloud computing is a \_\_\_\_\_ system and it is necessarily unidirectional in nature.

- A. stateless
- B. stateful
- C. reliable
- D. all of the mentioned

102. Which of the following is the most important area of concern in cloud computing?





- A. Security
- B. Storage
- C. Scalability
- D. All of the mentioned

103. You can't count on a cloud provider maintaining your \_\_\_\_\_ in the face of government actions.

- A. scalability
- B. reliability
- C. privacy
- D. none of the mentioned

104. Which of the following architectural standards is working with cloud computing industry?

- A. Service-oriented architecture
- B. Standardized Web services
- C. Web-application frameworks
- D. All of the mentioned

105. The information that gets transformed in encryption is \_\_\_\_\_

- A. Plain text
- B. Parallel text
- C. Encrypted text
- D. Decrypted text

106. Which is not an objective of network security?

- A. Identification
- B. Authentication
- C. Access control
- D. Lock

107. Which of these is a part of network identification?





- A. UserID
- B. Password
- C. OTP
- D. fingerprint

108. The process of verifying the identity of a user.

- A. Authentication
- B. Identification
- C. Validation
- D. Verification

109. An algorithm in encryption is called \_\_\_\_\_

- A. Algorithm
- B. Procedure
- C. Cipher
- D. Module

110. The information that gets transformed in encryption is \_\_\_\_\_

- A. Plain text
- B. Parallel text
- C. Encrypted text
- D. Decrypted text

112. The field that covers a variety of computer networks, both public and private, that are used in everyday jobs.

- A. Artificial Intelligence
- B. ML
- C. Network Security
- D. IT

113. Network Security provides authentication and access control for resources.

- A. True

B. False

**114. Which is not an objective of network security?**

- A. Identification
- B. Authentication
- C. Access control
- D. Lock

**115. Which of these is a part of network identification?**

- A. UserID
- B. Password
- C. OTP
- D. fingerprint

**116. An algorithm in encryption is called \_\_\_\_\_**

- A. Algorithm
- B. Procedure
- C. Cipher
- D. Module

**117. A data warehouse is which of the following?**

- A. Can be updated by end users.
- B. Contains numerous naming conventions and formats.
- C. Organized around important subject areas.
- D. Contains only current data.

**118. An operational system is which of the following?**

- A. A system that is used to run the business in real time and is based on historical data.
- B. A system that is used to run the business in real time and is based on current data.
- C. A system that is used to support decision making and is based on current data.
- D. A system that is used to support decision making and is based on historical data



119. A goal of data mining includes which of the following?

- A. To explain some observed event or condition
- B. To confirm that data exists
- C. To analyze data for expected relationships
- D. To create a new data warehouse

120. Data transformation includes which of the following?

- A. A process to change data from a detailed level to a summary level
- B. A process to change data from a summary level to a detailed level
- C. Joining data from one source into various sources of data
- D. Separating data from one source into various sources of data



81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
D	D	A	C	B	D	A	A	D	A	C	D	A	A	D	C	A	B	A	B
101	102	103	104	105	106	107	108	108	109	110	111	112	113	114	115	116	117	118	120
A	A	C	A	A	D	A	A	A	C	C	C	C	A	D	A	C	C	B	A

**121. The extract process is which of the following?**

- A. Capturing all of the data contained in various operational systems
- B. Capturing a subset of the data contained in various operational systems
- C. Capturing all of the data contained in various decision support systems
- D. Capturing a subset of the data contained in various decision support systems

**122.A star schema has what type of relationship between a dimension and fact table?**

- A. Many-to-many
- B. One-to-one
- C. One-to-many
- D. All of the above.

**123 Transient data is which of the following?**

- A. Data in which changes to existing records cause the previous version of the records to be eliminated
- B. Data in which changes to existing records do not cause the previous version of the records to be eliminated
- C. Data that are never altered or deleted once they have been added
- D. Data that are never deleted once they have been added

**124 A multifold transformation does which of the following?**

- A. Converts data from one field into multiple fields
- B. Converts data from multiple fields into one field
- C. Converts data from multiple fields into multiple fields
- D. All of the above

**125. \_\_\_\_\_ computing refers to applications and services that run on a distributed network using virtualized resources.**





- A. Distributed
- B. Cloud
- C. Soft
- D. Parallel

126. Point out the wrong statement.

- A. The massive scale of cloud computing systems was enabled by the popularization of the Internet
- B. Soft computing represents a real paradigm shift in the way in which systems are deployed
- C. Cloud computing makes the long-held dream of utility computing possible with a pay-as-you-go, infinitely scalable, universally available system
- D. All of the mentioned

127. \_\_\_\_\_ as a utility is a dream that dates from the beginning of the computing industry itself.

- A. Model
- B. Computing
- C. Software
- D. All of the mentioned

128. Which of the following is essential concept related to Cloud?

- A. Reliability
- B. Productivity
- C. Abstraction
- D. All of the mentioned

129. Which of the following can be identified as cloud?

- A. Web Applications
- B. Intranet
- C. Hadoop
- D. All of the mentioned





130. Cloud computing is an abstraction based on the notion of pooling physical resources and presenting them as a \_\_\_\_\_ resource.

- A. real
- B. virtual
- C. cloud
- D. none of the mentioned

131. \_\_\_\_\_ has many of the characteristics of what is now being called cloud computing.

- A. Internet
- B. Softwares
- C. Web Service
- D. All of the mentioned

132. Which of the following is Cloud Platform by Amazon?

- A. Azure
- B. AWS
- C. Cloudera
- D. All of the mentioned

133. All cloud computing applications suffer from the inherent \_\_\_\_\_ that is intrinsic in their WAN connectivity.

- A. propagation
- B. latency
- C. noise
- D. all of the mentioned

134. Which of the following is the most important area of concern in cloud computing?

- A. Security
- B. Storage
- C. Scalability
- D. All of the mentioned

135. Which of the following architectural standards is working with cloud computing industry?

- A. Service-oriented architecture
- B. Standardized Web services

- C. Web-application frameworks
- D. All of the mentioned

**136. Point out the wrong statement.**

- A. Everything from the application down to the infrastructure is the vendor's responsibility
- B. In the deployment model, different cloud types are an expression of the manner in which infrastructure is deployed
- C. AaaS provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures
- D. All of the mentioned

**137. Which of the following is not a diagram studied in Requirement Analysis ?**

- A. Use Cases
- B. Entity Relationship Diagram
- C. State Transition Diagram
- D. Activity Diagram

**138.How many feasibility studies is conducted in Requirement Analysis ?**

- A. Two
- B. Three
- C. Four
- D. None of the mentioned.

**139. How many phases are there in Requirement Analysis ?**

- A. Three
- B. Four
- C. Five
- D. Six

**140. Requirements analysis is critical to the success of a development project.**

- A. True

- B. False
- C. Depends upon the size of project
- D. None of the mentioned

**141. Requirements Analysis is an Iterative Process.**

- A. True
- B. False.

**142. Coad and Yourdon suggested \_\_\_\_\_ selection characteristics that should be used as an analyst considers each potential object for inclusion in the requirement analysis model.**

- A. Three
- B. Four
- C. Five
- D. Six

**143. Requirements should specify 'what' but not 'how'.**

- A. True
- B. False

**144. Which of the following property does not correspond to a good Software Requirements Specification (SRS) ?**

- A. Verifiable
- B. Ambiguous
- C. Complete
- D. Traceable

**145. In size oriented metrics, metrics are developed based on the \_\_\_\_\_**

- A. number of Functions
- B. number of user inputs
- C. number of lines of code
- D. amount of memory usage

**146. Defects removal efficiency (DRE) depends on:**

- A. E – errors found before software delivery
- B. D – defects found after delivery to user
- C. Both E and D
- D. Varies with project

**147. Size and Complexity are a part of**

- A. Product Metrics
- B. Process Metrics
- C. Project Metrics
- D. All of the mentioned

**148. Cost and schedule are a part of**

- A. Product Metrics
- B. Process Metrics
- C. Project Metrics
- D. All of the mentioned

**149. Number of errors found per person hours expended is an example of a**

- A. measurement
- B. measure
- C. metric
- D. all of the mentioned

**150. Which of the following is not categorized under Product Operation of McCall's Software Quality Factors?**

- A. Flexibility
- B. Reliability
- C. Usability
- D. Integrity

**151 Which of the following is not categorized under Component-Level Design Metrics?**

- A. Complexity Metrics
- B. Cohesion Metrics



- C. Morphology Metrics
- D. Coupling Metrics

**152. Number of phases in the handshaking protocol?**

- A. 2
- B. 3
- C. 4
- D. 5

**153 Which of the following slows the cryptographic algorithm –**

- 1) Increase in Number of rounds
- 2) Decrease in Block size
- 3) Decrease in Key Size
- 4) Increase in Sub key Generation

- A. 1 and 3
- B. 2 and 3
- C. 3 and 4
- D. 2 and 4

**154. n brute force attack, on average half of all possible keys must be tried to achieve success.**

- A. True
- B. False

**155. If the sender and receiver use different keys, the system is referred to as conventional cipher system.**

- A. True
- B. False

**156.The time required to convert a k-bit integer to its representation in the base 10 in terms of big-O notation is**

- A.  $O(\log_2 n)$





- B.  $O(\log n)$
- C.  $O(\log^2 2n)$
- D.  $O(2\log n)$

157.An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available.

- A. True
- B. False

158. What is the size of the key in the SDES algorithm?

- A. 24 bits
- B. 16 bits
- C. 20 bits
- D. 10 bits

159.Assume input 10-bit key, K: 101000010 for the SDES algorithm. What is K1?

- A. 10100100
- B. 01011011
- C. 01101000
- D. 10100111

160. Use Caesar’s Cipher to decipher the following

HQFUBSWHG WHAW

- A. ABANDONED LOCK
  - B. ENCRYPTED TEXT
  - C. ABANDONED TEXT
  - D. ENCRYPTED LOCK
- Answer Key

121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
B	C	A	D	B	B	B	C	C	B	A	B	B	A	A	C	D	B	C	A
141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
A	D	A	B	C	C	A	C	C	A	C	C	B	A	B	A	A	D	A	B

161. Caesar Cipher is an example of

- A. Poly-alphabetic Cipher
- B. Mono-alphabetic Cipher
- C. Multi-alphabetic Cipher
- D. Bi-alphabetic Cipher

162. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

- A. True
- B. False

163. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.

- A. Random Polyalphabetic, Plaintext, Playfair
- B. Random Polyalphabetic, Playfair, Vignere
- C. Random Polyalphabetic, Vignere, Playfair, Plaintext
- D. Random Polyalphabetic, Plaintext, Beaufort, Playfair

164. On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-

- A. abqdnwewujphfvrrrfznsdokvl
- B. abqdvwmwujphfvvyrfznydokvl
- C. tbqyrvmwujphfvvyrfznydokvl
- D. baiuvmwujphfoeirfznydokvl

165. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text

- A. nlazeiiblji
- B. nlazeiibljii
- C. olaaeiibljki
- D. mlaaeiibljki

166. A symmetric cipher system has an IC of 0.041. What is the length of the key ‘m’?

- A. 1
- B. 3
- C. 2

## D. 5

167. AES uses a \_\_\_\_\_ bit block size and a key size of \_\_\_\_\_ bits.

- A. 128; 128 or 256
- B. 64; 128 or 192
- C. 256; 128, 192, or 256
- D. 128; 128, 192, or 256

168. There is an addition of round key before the start of the AES round algorithms.

- A. True
- B. False

169. Which of the 4 operations are false for each round in the AES algorithm

- i) Substitute Bytes
- ii) Shift Columns
- iii) Mix Rows
- iv) XOR Round Key

- A. only
- B. iii) and iv)
- C. and iii)
- D. only iv)

170 Conversion of the Plaintext MANIPALINSTITUTE to a state matrix leads to a)

M	A	N	I
P	A	L	I
N	S	T	I
T	U	T	E

b)



M	P	N	T
A	A	S	U
N	L	T	T
I	I	I	E

c)

M	A	I	L
N	P	I	T
A	N	I	U
S	T	T	E

d)

E	U	T	L
T	I	I	L
T	N	P	A
S	A	N	M

171.On encrypting MANIPALINSTITUTE with key ADVANCEDENCRYPTI we get the state matrix –

a)

FC	1D	1B	0D
15	02	1D	05
10	0F	17	00
20	0D	1B	FC



b)

FC	1D	1B	0D
15	02	1D	05
10	0F	17	00
20	0D	1B	0C

c)

OC	FE	0B	0D
D5	02	1D	05
18	09	17	00
08	0D	1B	FC

d)

OC	1E	0B	0D
05	02	1D	05
18	09	17	00
08	0D	1B	0C

172 The \_\_\_\_\_ model originally did not require a cloud to use virtualization to pool resources.

- A. NEFT
- B. NIST
- C. NIT
- D. All of the mentioned





173. Wi-Fi stands for-

- A. Wireless Fidelity
- B. Wireless LAN
- C. Wireless FLAN
- D. None of the mentioned

174. Wired networks are far more susceptible to eavesdropping and jamming than wireless networks.

- A. True
- B. False

175. “A user intending to connect to one LAN may unintentionally lock onto a wireless access point from the neighboring network.” Which type of Wireless network threat would you classify this under?

- A. Malicious Threat
- B. Network Injection
- C. Denial Of Service
- D. Accidental Association

176. “When there is a lack of a central point of control.” Which type of Wireless network threat would you classify this under?

- A. Man in the middle attack
- B. Identity Theft
- C. Ad Hoc Networks
- D. Non-Traditional Networks

177. “When fraud access points are created to access information such as passwords.” Which type of Wireless network threat would you classify this under?

- A. Identity Theft
- B. Network Injection
- C. Man in the middle attack
- D. Malicious Association



178. “When bogus reconfiguration commands are used to affect routers and switches to degrade network performance.” Which type of Wireless network threat would you classify this under?

- A. Network Injection
- B. Malicious Association
- C. Man in the middle attack
- D. Denial Of Service

179. “When communication is unknowingly going through an adversary/intermediate.” Which type of Wireless network threat would you classify this under?

- A. Malicious Association
- B. Man in the middle attack
- C. Network Injection
- D. Accidental Association

180. “When an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.” Which type of Wireless network threat would you classify this under?

- A. Identity Theft.
- B. Man in the middle attack
- C. Network Injection
- D. Accidental Association

181. SSID stands for –

- A. Secure Service Identifier
- B. Secure Set Independent Device
- C. Secure Set Identifier
- D. Service Set Independent Device



**182. Mobile Device security falls under 3 categories. Which of these is not a valid Mobile Device security category?**

- A. Barrier security
- B. Traffic security
- C. Device security
- D. All of the above

**183 “Installation of third party applications are prohibited on many company hardware devices such as laptops, mobiles, etc.” Which Mobile Device security category of implementation does this fall under?**

- A. Barrier security
- B. Traffic security
- C. Device security
- D. None of the mentioned

**184. VPN stands for –**

- A. Visual Performance Node
- B. Virtual Private Network
- C. Virtual Post Node
- D. Virtual Post Network

**185. Another name for the Wireless Ethernet 802.11a is-**

- A. Wi-Fi
- B. Wi-Fi4
- C. Wi-Fi5
- D. Wi-Fi6

**186. Which of these is not a valid Signal-Hiding Technique for Wireless networks?**

- A. reducing the signal strength to the lowest level such that it still provides requisite coverage
- B. using directional antennas and signal shielding techniques
- C. installing the wireless access point away from exteriors of the building
- D. none of the mentioned

**187. Caesar Cipher is an example of**

- A. Poly-alphabetic Cipher



- B. Mono-alphabetic Cipher
- C. Multi-alphabetic Cipher
- D. Bi-alphabetic Cipher

**188. On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-**

- A. abqdnwewuwjphfvrrtrfznsdokvl
- B. abqdvmmuwjphfvvyyrfznydokvl
- C. tbqyrvmmuwjphfvvyyrfznydokvl
- D. baiuvmuwjphfoeiyrfznydokvl

**189. How many modes of operation are there in in DES and AES?**

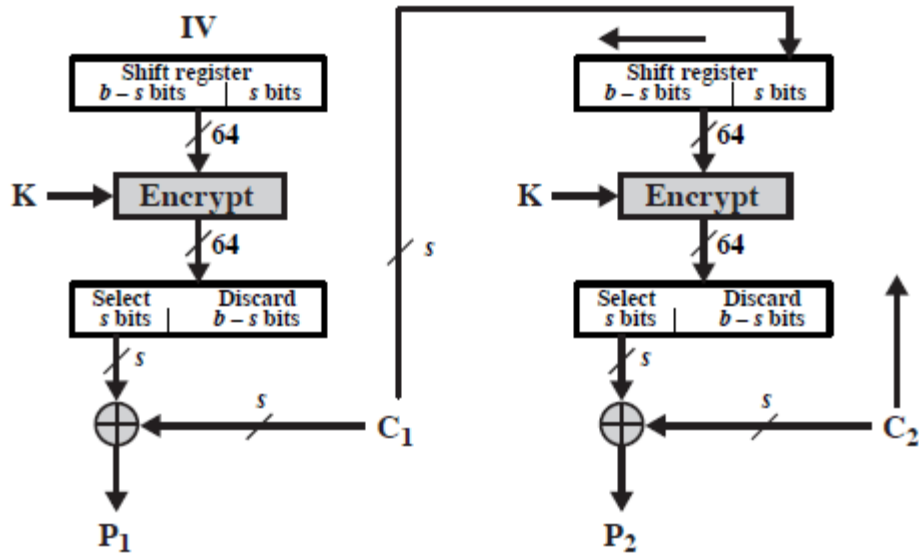
- A. 4
- B. 3
- C. 2
- D. 5

**190. Which one of the following modes of operation in DES is used for operating short data?**

- A. Cipher Feedback Mode (CFB)
- B. Cipher Block chaining (CBC)
- C. Electronic code book (ECB)
- D. Output Feedback Modes (OFB)



191 . What is the fault in the above figure?



- a) The output of the XOR is sent to the next stage
- b) The “Encrypt” Box should be replaced by “Decrypt Box
- c) b-s bits are selected for the XOR operation
- d) No fault

192 During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.

- A. True
- B. False

193. A preferable cryptographic algorithm should have a good avalanche effect.

- A. True
- B. False

194. The number of tests required to break the Double DES algorithm are

- A. 2112
- B. 2111
- C. 2128
- D. 2119





195 How many keys does the Triple DES algorithm use?

- A. 2
- B. 3
- C. 2 or 3
- D. 3 or 4

196. In triple DES, the key size is \_\_\_ and meet in the middle attack takes \_\_\_ tests to break the key.

- A. 2192 ,2112
- B. 2184,2111
- C. 2168,2111
- D. 2168,2112

197. When a hash function is used to provide message authentication, the hash function value is referred to as

- A. Message Field
- B. Message Digest**
- C. Message Score
- D. Message Leap

198. Message authentication code is also known as

- A. key code
- B. hash code
- C. keyed hash function**
- D. message key hash function

199. Which one of the following is not an application hash functions?

- A. One-way password file
- B. Key wrapping
- C. Virus Detection
- D. Intrusion detection

200 A larger hash code cannot be decomposed into independent subcodes.

- A. True
- B. False



161	162	163	164	165	166	167	168	19	170	171	172	173	174	175	176	177	178	179	180
B	B	C	B	A	D	D	A	B	B	D	B	A	B	D	C	D	A	B	A
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200
C	D	C	B	C	D	B	B	D	C	B	A	A	B	C	D	B	C	A	B





