Roll No. .....

Question Booklet Number

O. M. R. Serial No. | | | | | | | | |

B. C. A. (Sixth Semester) EXAMINATION, 2022-23

COMPUTER NETWORK SECURITY

Paper Code						
B	C	A	6	0	1	N

Questions Booklet Series
A

Time : 1:30 Hours] [*Maximum Marks : 75*

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 100 questions. Examinee is required to answer 75 questions in the OMR Answer-Sheet provided and not in the question booklet. All questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को 75 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, प्रश्न-पुस्तिका पर नहीं। सभी प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गए हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, तो उसे तुरन्त बदल लें।

(Remaining instructions on the last page) (शेष निर्देश अन्तिम पृष्ठ पर)

(Only for Rough Work)

1. What ensures the security of information and resources present in the website of the intranet ?

(A) security alarm

(B) firewall

(C) blocker

(D) malware

2. In a computing organization ..... is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

(A) spyware

(B) cookies

(C) spam

(D) firewall

3. A computer virus is a :

(A) software

(B) hardware

(C) bacteria

(D) freeware

4. ..... uses PGP application.

(A) Email

(B) File encryption

(C) E-mail and file encryption

(D) None of the above

5. A digital signature is required :

(A) for all e-mail sent

(B) for all FTP transaction

(C) for non-repudiation of communication by sender

(D) None of the above

6. Unsolicited electronic message sent for marketing purpose are called :

(A) virus

(B) zip

(C) spam

(D) URL

7. What does DDOS stand for ?

(A) Denial Data of Service

(B) Denial Distributed of Service

(C) Distributed Denial of Service

(D) Distribution of Data Service

8. PGP stands for :

(A) Proper Good Privacy

(B) Privacy Good Principle

(C) Pretty Good Privacy

(D) None of the above

9. PGP may use ....., ... cipher per message authentication and encryption respectively.

(A) IDEA, DES

(B) RSA, Triple DES

(C) Triple DES, RSA

(D) RSA, Deffie-Hellman

10. ..... is used for network level security.

(A) IPSEC

(B) SSL

(C) TLS

(D) SET

11. Full form of SET is :

(A) Security of E-mail Transaction

(B) Secure Electronic Transaction

(C) Select Electronic Type

(D) None of the above

12. For distribution of public key, which of the following uses trusted third party interface ?

(A) Public announcement

(B) Publicly available directory

(C) Public key certificate

(D) None of the above

13. For message authentication, i.e. integrity of message, which mechanism is used ?

(A) MAC

(B) IPSEC

(C) TLS

(D) SET

14. Kerberos is used for :

(A) Authentication and client-server environment

(B) Authentication of e-mail

(C) Confidentiality of message

(D) None of the above

15. A ..... is an extension of an enterprise's private intranet across a public network such as the internet, creating a secure private connection.

(A) VNP

(B) VAN

(C) VPN

(D) VSPN

16. Which of the following statements is NOT true concerning VPNs ?

(A) Is the backbone of the Internet.

(B) Allows remote workers to access corporate data.

(C) Allows LAN-to-LAN connectivity over public networks.

(D) Financially rewarding compared to leased lines.

17. Which component is included in IP security ?

(A) Authentication Header (AH)

(B) Encapsulating Security Payload (ESP)

(C) Internet Key Exchange (IKE)

(D) All of the mentioned

18. Threat on availability of computer resource to its intended users is called ..... .

(A) Denial-of-service attack

(B) Virus attack

(C) Worms attack

(D) Botnet process

19. PGP encrypts data by using a block cipher is called ..... .

(A) Private data encryption algorithm

(B) International data encryption algorithm

(C) Internet data encryption algorithm

(D) Local data encryption algorithm

20. Which is not an objective of network security ?

(A) Secrecy

(B) Authentication

(C) Access control

(D) Lock and unlock

21. The process of verifying the identity of a user :

(A) Identification

(B) Authentication

(C) Validation

(D) Verification

22. The secure authentication connection is known as :

(A) chisel

(B) handshaking

(C) tunnel

(D) zeroing

23. In which of the following there is continuous surveillance on target by another group of people ?

(A) phishing

(B) stalking

(C) identity crisis

(D) bullying

24. Which of these is considered as unsolicited e-mail ?

(A) virus

(B) malware

(C) bacteria

(D) spam

25. ..... is a software to help the user computer detect virus.

(A) Malware

(B) Antivirus

(C) Adware

(D) None of the above

26. Which of these refers to verifying the integrity of message ?

(A) digital signature

(B) message digest

(C) protocol

(D) decryption algo

27. In system hacking, which of these is most important activity ?

(A) information gathering

(B) covering tracks

(C) cracking password

(D) None of the above

28. Which of these can be considered as the element of cyber security ?

(A) Application security

(B) Operational security

(C) Network security

(D) All of the above

29. In the computer network, the encryption techniques is mainly used for improving :

(A) security

(B) performance

(C) reliability

(D) longevity

30. Cryptanalysis is used ..... .

(A) to find some insecurity in a cryptographic scheme

(B) to increase the speed

(C) to encrypt the data

(D) to make new ciphers

31. Which two types of encryption protocols can be used to secure the authentication of computers using IPsec ?

(A) Kerberos V5

(B) SHA

(C) MD5

(D) Both SHA and MD5

32. Which two types of IPsec can be used to secure communications between two LANs ?

(A) AH tunnel mode

(B) ESP tunnel mode

(C) Both AH tunnel mode and ESP tunnel mode

(D) ESP transport mode

33. ESP does not provide ..... .

(A) source authentication

(B) data integrity

(C) privacy

(D) error control

34. IP Security operates in which layer of the OSI model ?

(A) Network

(B) Transport

(C) Application

(D) Physical

35. Which of the following is not a type of symmetric key cryptographic technique ?

(A) Caeser cipher

(B) Data Encryption Standard

(C) Playfair cipher

(D) Diffie Hellman cipher

36. Which of the following is a passive attack ?

(A) Masquerade

(B) Modification of message

(C) Denial of service

(D) Traffic analysis

37. A mechanism used to encrypt and decrypt data is known as :

(A) cryptanalysis

(B) cryptography

(C) Both (A) and (B)

(D) None of the above

38. Conventional encryption and public key encryption are also called ..... and ..... respectively.

(A) asymmetric encryption, symmetric encryption

(B) symmetric encryption, asymmetric encryption

(C) two-key encryption, one-key encryption

(D) None of the above

39. Which of the following combination is symmetric encryption techniques ?

(A) DES, RSA, Diffie-Hellman

(B) MD5, SHA-2, DSS

(C) IDEA, CAST, TRIPLE DES

(D) DSS, IDEA, SHA-1

40. Which is the type of text that is transformed by a cipher at the receiver side ?

(A) plaintext

(B) cipher text

(C) error text

(D) scalar text

41. Which of the following malware does not replicate through infection ?

(A) rootkit

(B) trojan

(C) virus

(D) worm

42. Which of the following is a independent malicious program that never requires any host program ?

(A) trojan horse

(B) worm

(C) trap door

(D) virus

43. Why are the factors like confidentiality, authentication, integrity availability considered as fundamental services ?

(A) to understand hacking process

(B) to understand elements of security breech

(C) to understand security and its component ib better way

(D) None of the above

44. In order to ensure the security of data, we need to ..... data.

(A) decrypt

(B) encrypt

(C) delete

(D) zip

45. RSA ..... be used for digital sign.

(A) must not

(B) can

(C) cannot

(D) should not

46. A digital signature is :

(A) a unique id of sender

(B) an authorization string for electronic record by binding with private key of sender

(C) encryption using public key of sender

(D) None of the above

47. A digital signature uses ..... system of cryptography.

(A) asymmetric key

(B) symmetric key

(C) secret key

(D) Both (A) and (B)

48. Digital signature scheme cannot provide :

(A) confidentiality

(B) authentication

(C) integrity

(D) None of the above

49. ..... is used to create digital signature.

(A) Public key of receiver

(B) Public key of sender

(C) Private key of sender

(D) Private key of receiver

50. ..... is used to verify digital signature.

(A) Public key of receiver

(B) Public key of sender

(C) Private key of sender

(D) Private key of receiver

51. Digital signature provides ..... .

(A) authentication

(B) non-repudiation

(C) Both (A) and (B)

(D) None of the above

52. In term of web security threat, impersonation of another user is :

(A) an active attack

(B) a passive attack

(C) Both (A) and (B)

(D) None of the above

53. Which one is not a protocol of SSL ?

(A) record

(B) handshake

(C) alarm

(D) change cipher

54. Full form of SSL is :

(A) Serial Session Layer

(B) Secure Session Layer

(C) Secure Socket Layer

(D) Secure Secure Layer

55. Which protocol is used to give error warning to peer entity ?

(A) record

(B) handshake

(C) alert

(D) change cipher

56. Which protocol is used for changing pending state to current state ?

(A) alert

(B) handshake

(C) record

(D) change cipher spec

57. IPSec is designed to provide security at :

(A) application level

(B) transport layer

(C) network layer

(D) session layer

58. In tunnel mode, IPSec protect the :

(A) IP header

(B) Entire IP packet

(C) IP payload

(D) None of the above

59. Denial of service attack is a threat to :

(A) confidentiality

(B) authentication

(C) availability

(D) access control

60. Conventional cryptography is also known as ..... or symmetric-key encryption.

(A) public key

(B) protected key

(C) secret key

(D) primary key

61. ..... cryptography is based on publicly known mathematically designed algorithms to encrypt the information.

(A) Modern

(B) Classic

(C) Traditional

(D) Primitive

62. Cryptography can be divided into ..... types.

(A) 5

(B) 4

(C) 3

(D) 2

63. When plaintext is converted to unreadable format, it is termed as ..... .

(A) rotten text

(B) raw text

(C) cipher-text

(D) ciphen-text

64. ..... is the process or mechanism used for converting ordinary plaintext into garbled non-human readable text and vice-versa.

(A) Malware analysis

(B) Exploit writing

(C) Cryptography

(D) Reverse engineering

65. Which one of the following algorithms is not used in asymmetric-key cryptography ?

(A) RSA algorithm

(B) Diffie-Helman algorithm

(C) Electronic code book algorithm

(D) DSA algorithm

66. PGP is used in :

(A) FTP security

(B) e-mail security

(C) browser security

(D) server security

67. IDEA is a/an :

(A) symmetric cipher

(B) asymmetric cipher

(C) authentication algo

(D) None of the above

68. For a client-server authentication, the client requests from a KDC a ..... for access to specific asset.

(A) ticket

(B) user

(C) token

(D) card

69. Message ..... means that data must arrive at the receiver as exactly sent.

(A) integrity

(B) confidentiality

(C) authentication

(D) None of the above

70. ..... means that sender must not deny of sending the message.

(A) Non-repudiation

(B) Non-sensing

(C) Confidentiality

(D) Availability

71. ..... function creates a message digest of a message.

(A) Encryption

(B) Hash

(C) Decryption

(D) None of the above

72. A(n) ..... is a govt. authorised organization that binds a public key to an entity and issues a certificate.

(A) KDC

(B) CA

(C) Kerberos

(D) None of the above

73. The ..... criteria says that it is almost impossible to create a message if message digest is known.

(A) one wayness

(B) strong collison resistancee

(C) weak collison

(D) None of the above

74. The criteria of hash that says we cannot find two message that has same message digest is :

(A) one wayness

(B) strong collison resistance

(C) weak collison resistance

(D) None of the above

75. Which application level protocol uses few manager controlling a set of agents ?

(A) HTML

(B) SNMP

(C) TCP

(D) All of the above

76. The main difference between SNMP V2 and SNMP V3 :

(A) classification

(B) increased security

(C) management

(D) integration

77. SNMP means :

(A) secure network management protocol

(B) set network management protocol

(C) simple network management protocol

(D) None of the above

78. SNMP is the framework for managing devices in the internet using :

(A) TCP/IP

(B) UDP

(C) SNP

(D) SMTP

79. ..... ensures the integrity and security of data that pass over network.

(A) Penetrating tool

(B) Firewall

(C) Network security protocol

(D) Antivirus

80. SSL primarily focuses on :

(A) integrity and non-repudiation

(B) integrity and authenticity

(C) authentication and privacy

(D) confidentiality and integrity

81. ..... theory is very important for success of RSA algo.

(A) Integer

(B) Prime no

(C) Random no

(D) Fraction

82. The SET protocol is used for :

(A) credit card payment

(B) cheque payement

(C) debit card payement

(D) None of the above

83. In SET protocol, a customer encrypts credit card no using :

(A) his private key

(B) bank private key

(C) bank public key

(D) merchnat public key

84. In SET, customer sends a purchase order :

(A) encrypted with his public key

(B) in plaintext

(C) using secure digital signature system

(D) using bank public key

85. SET uses ..... for secure payment info and purchase order.

(A) encryption

(B) dual signature

(C) MAC

(D) hashing

86. In network management system, the predefined policy to control to access to network is called :

(A) fault management

(B) security management

(C) active management

(D) passive management

87. Communication between end system is encrypted using a key, known as :

(A) session key

(B) temporary key

(C) public key

(D) private key

88. In cryptography, cipher means :

(A) algo for encryption

(B) algo for encryption and decryption

(C) encrypted message

(D) decrypted message

89. In asymmetric key cryptography, for confidentiality, the private key of ..... is used.

(A) receiver

(B) sender

(C) Both sender and receiver

(D) None of the above

90. In asymmetric key cryptography, for authentication, the public key of ..... is used.

(A) receiver

(B) sender

(C) Both sender and receiver

(D) None of the above

91. Which is not an asymmetric key cryptography ?

(A) RSA

(B) Diffie-Hellman

(C) DSS

(D) IDEA

92. What is data encryption standard DES ?

(A) block cipher

(B) stream cipher

(C) asymmeric cipher

(D) string cipher

93. Caesar cipher is :

(A) propositional cipher

(B) substitution cipher

(C) permutation cipher

(D) transposition cipher

94. In cryptography, changing order of letter in message is :

(A) transpositional cipher

(B) substitution cipher

(C) Both (A) and (B)

(D) Diffie-Hellman algo

95. Cryptanalysis is used to :

(A) find key or plaintext or both of the cryptographic scheme

(B) encrypt data

(C) make new cipher

(D) None of the above

96. Which of the following protocols is used to secure HTTP connection ?

(A) IPSec

(B) TLS

(C) ECN

(D) FTP

97. Cryptographic hash function takes an arbitrary block of data and returns :

(A) variable size byte stream

(B) variable size bit stream

(C) fixed size bit stream

(D) None of the above

98. An asymmetric key cipher uses :

(A) 2 keys

(B) 3 keys

(C) 1 key

(D) 4 keys

99. DES uses :

(A) 56 bit block, 64 bit key

(B) 56 bit block, 56 bit key

(C) 64 bit block, 64 bit key

(D) 64 bit block, 56 bit key

100. DES uses ..... rounds of fiestel cipher structure.

(A) 8

(B) 12

(C) 16

(D) 32

4. Four alternative answers are mentioned for each question as—A, B, C & D in the booklet. The candidate has to choose the correct answer and mark the same in the OMR Answer-Sheet as per the direction :

Example :

Question :

Q. 1 (A) ● (C) (D)
Q. 2 (A) (B) ● (D)
Q. 3 (A) ● (C) (D)

Illegible answers with cutting and over-writing or half filled circle will be cancelled.

5. Each question carries equal marks. Marks will be awarded according to the number of correct answers you have.

6. All answers are to be given on OMR Answer sheet only. Answers given anywhere other than the place specified in the answer sheet will not be considered valid.

7. Before writing anything on the OMR Answer Sheet, all the instructions given in it should be read carefully.

8. After the completion of the examination candidates should leave the examination hall only after providing their OMR Answer Sheet to the invigilator. Candidate can carry their Question Booklet.

9. There will be no negative marking.

10. Rough work, if any, should be done on the blank pages provided for the purpose in the booklet.

11. To bring and use of log-book, calculator, pager and cellular phone in examination hall is prohibited.

12. In case of any difference found in English and Hindi version of the question, the English version of the question will be held authentic.

Impt. : On opening the question booklet, first check that all the pages of the question booklet are printed properly. If there is ny discrepancy in the question Booklet, then after showing it to the invigilator, get another question Booklet of the same series.

4. प्रश्न-पुस्तिका में प्रत्येक प्रश्न के चार सम्भावित उत्तर— A, B, C एवं D हैं। परीक्षार्थी को उन चारों विकल्पों में से सही उत्तर छाँटना है। उत्तर को OMR आन्सर-शीट में सम्बन्धित प्रश्न संख्या में निम्न प्रकार भरना है :

उदाहरण :

प्रश्न :

प्रश्न 1 (A) ● (C) (D)
प्रश्न 2 (A) (B) ● (D)
प्रश्न 3 (A) ● (C) (D)

अपठनीय उत्तर या ऐसे उत्तर जिन्हें काटा या बदला गया है, या गोले में आधा भरकर दिया गया, उन्हें निरस्त कर दिया जाएगा।

5. प्रत्येक प्रश्न के अंक समान हैं। आपके जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।

6. सभी उत्तर केवल ओ. एम. आर. उत्तर-पत्रक (OMR Answer Sheet) पर ही दिये जाने हैं। उत्तर-पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।

7. ओ. एम. आर. उत्तर-पत्रक (OMR Answer Sheet) पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाये।

8. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी OMR Answer Sheet उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें। परीक्षार्थी अपने साथ प्रश्न-पुस्तिका ले जा सकते हैं।

9. निगेटिव मार्किंग नहीं है।

10. कोई भी रफ कार्य, प्रश्न-पुस्तिका के अन्त में, रफ-कार्य के लिए दिए खाली पेज पर ही किया जाना चाहिए।

11. परीक्षा-कक्ष में लॉग-बुक, कैलकुलेटर, पेजर तथा सेल्युलर फोन ले जाना तथा उसका उपयोग करना वर्जित है।

12. प्रश्न के हिन्दी एवं अंग्रेजी रूपान्तरण में भिन्नता होने की दशा में प्रश्न का अंग्रेजी रूपान्तरण ही मान्य होगा।

महत्वपूर्ण : प्रश्नपुस्तिका खोलने पर प्रथमतः जाँच कर देख लें कि प्रश्न-पुस्तिका के सभी पृष्ठ भलीभाँति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्षनिरीक्षक को दिखाकर उसी सिरीज की दूसरी प्रश्न-पुस्तिका प्राप्त कर लें।