Roll No.----------

Paper Code		
3	7	7

(To be filled in the OMR Sheet)

प्रश्नपुस्तिका क्रमांक
Question Booklet No.

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

प्रश्नपुस्तिका सीरीज
Question Booklet Series

A

BCA (Sixth Semester) Examination, July-2022

BCA-601(N)

Computer Network Security

Time : 1:30 Hours **Maximum Marks-100**

जब तक कहा न जाय, इस प्रश्नपुस्तिका को न खोलें

निर्देश : –

1. परीक्षार्थी अपने अनुक्रमांक, विषय एवं प्रश्नपुस्तिका की सीरीज का विवरण यथास्थान सही– सही भरें, अन्यथा मूल्यांकन में किसी भी प्रकार की विसंगति की दशा में उसकी जिम्मेदारी स्वयं परीक्षार्थी की होगी।
2. **इस प्रश्नपुस्तिका में 100 प्रश्न हैं, जिनमे से केवल 75 प्रश्नों के उत्तर परीक्षार्थियों द्वारा दिये जाने है। प्रत्येक प्रश्न के चार वैकल्पिक उत्तर प्रश्न के नीचे दिये गये हैं। इन चारों में से केवल एक ही उत्तर सही है। जिस उत्तर को आप सही या सबसे उचित समझते हैं, अपने उत्तर पत्रक (O.M.R. ANSWER SHEET) में उसके अक्षर वाले वृत्त को काले या नीले बाल प्वांइट पेन से पूरा भर दें। यदि किसी परीक्षार्थी द्वारा किसी प्रश्न का एक से अधिक उत्तर दिया जाता है, तो उसे गलत उत्तर माना जायेगा।**
3. प्रत्येक प्रश्न के अंक समान हैं। आप के जितने उत्तर सही होंगे, उन्हीं के अनुसार अंक प्रदान किये जायेंगे।
4. सभी उत्तर केवल ओ०एम०आर० उत्तर पत्रक **(O.M.R. ANSWER SHEET)** पर ही दिये जाने हैं। उत्तर पत्रक में निर्धारित स्थान के अलावा अन्यत्र कहीं पर दिया गया उत्तर मान्य नहीं होगा।
5. ओ०एम०आर० उत्तर पत्रक **(O.M.R. ANSWER SHEET)** पर कुछ भी लिखने से पूर्व उसमें दिये गये सभी अनुदेशों को सावधानीपूर्वक पढ़ लिया जाय।
6. परीक्षा समाप्ति के उपरान्त परीक्षार्थी कक्ष निरीक्षक को अपनी ओ०एम०आर० शीट उपलब्ध कराने के बाद ही परीक्षा कक्ष से प्रस्थान करें।
7. निगेटिव मार्किंग नहीं है।

महत्वपूर्ण : – **प्रश्नपुस्तिका खोलने पर प्रथमतः जॉच कर देख लें कि प्रश्नपुस्तिका के सभी पृष्ठ भलीभॉति छपे हुए हैं। यदि प्रश्नपुस्तिका में कोई कमी हो, तो कक्ष निरीक्षक को दिखाकर उसी सीरीज की दूसरी प्रश्नपुस्तिका प्राप्त कर लें।**

K-377

Rough Work / रफ कार्य

1. Which of the following is a type of asymmetric key cryptographic technique ?

   (A) Playfair cipher

   (B) Deffie hellman cipher

   (C) DES

   (D) CAST

2. Which of the following is not a service of data security sent over network ?

   (A) Data confidentiality

   (B) Data integrity

   (C) Authentication

   (D) None of the above

3. Which of the following is not an active attack ?

   (A) Masquerade

   (B) Modification of message

   (C) Denial of service

   (D) Traffic analysis

4. Brute force attack means :

   (A) Brutally forcing the user to show useful info like pins and password

   (B) Trying every possible key to decrypt the message

   (C) One entity pretends to be some other entity

   (D) The message or info is modified before sending it to receiver

5. A mechanism to encrypt and decrypy data :

   (A) Ctyptography

   (B) Cryptology

   (C) Crypyanalysis

   (D) None of the above

6. The data encryption standard is an example of :

(A) Symmetric cipher

(B) Asymmetric cipher

(C) Logical cipher

(D) Standard algorithm

7. Public key cryptography is :

(A) Symmetric

(B) Asymmetric

(C) Both symmetric and asymmetric

(D) None of the above

8. For confidentiality, The private key, in asymmetric key cryptography, is used by :

(A) Sender

(B) Receiver

(C) Sender and receiver

(D) None

9. For Authentication, the private key, in public key cryptography, is used by :

(A) Sender

(B) Receiver

(C) All of the above

(D) None of the above

10. Which one of the following algorithm is not used as asymmetric-key cryptography ?

(A) RSA algorithm

(B) Diffie-Hellman algorithm

(C) Electronic code book algorithm

(D) DSS algorithm

11. In conventional cryptography, the order of the letters in a message is rearranged by_____.

(A) Transpositional ciphers

(B) Substitution ciphers

(C) Both Transpositional ciphers and Substitution ciphers

(D) Asymmetric ciphers

12. What is data encryption standard (DES) ?

(A) Block cipher

(B) Stream cipher

(C) Bit cipher

(D) Byte cipher

13. Cryptanalysis is used _____.

(A) To find some insecurity in a cryptographic scheme to get original message or key or both

(B) To increase the speed of execution

(C) To encrypt the data

(D) To make new ciphers

14. Cryptographic hash function takes an arbitrary block of data and returns _____.

(A) Fixed size bit string

(B) Variable size bit string

(C) Both fixed size bit string and variable size bit string

(D) Variable size byte string

15. RSA _____ be used for digital signature.

(A) Must not

(B) Cannot

(C) Can

(D) Must

16. A digital signature is :

(A) A bit string giving identity of a document/user

(B) A unique identification of a sender

(C) An authentication of an electronic record by binding it uniquely to a key only a sender knows

(D) An encrypted signature of sender

17. The key of a key pair used to verify a digital signature _____.

(A) Public key

(B) Private key

(C) Verifying key

(D) Secret key

18. Digital signature provides _____.

(A) Authentication, integrity

(B) Nonrepudiation, authentication

(C) Both (A) and (B)

(D) Neither (A) nor (B)

19. Using Kerberos, the client requests from the KDC a _____for access to a specific asset.

(A) Ticket

(B) Key

(C) Token

(D) Public key

20. Pretty Good Privacy (PGP) security system uses :

(A) Symmetric key cryptosystem

(B) Asymmetric key cryptosystem

(C) Symmetric & asymmetric key cryptosystem

(D) None of the mentioned

21. Public key cryptosystem is used for the encryption of :

(A) Messages

(B) Session key

(C) Session key & Messages

(D) None of the mentioned

22. PGP offers _____ block ciphers for message encryption.

(A) Triple-DES

(B) CAST

(C) IDEA

(D) All of the mentioned

23. The key size of DES is :

(A) 56 bits

(B) 64 bits

(C) 128 bits

(D) 168 bits

24. S/MIME stands for _____.

(A) Standard multipurpose internet mail extensions

(B) Secure multipurpose internet mail extensions

(C) Secure multipurpose international mail extensions

(D) Standard multipurpose international mail

25. The _____ acts as financial institutions who provides a payment card to a card holder.

(A) Payment gateway

(B) Card holder

(C) Acquirer

(D) Issuer

26. Who will be responsible for processing the payment from the customer's account to the merchant account ?

(A) Acquirer

(B) Certification authority

(C) Issuer

(D) Payment gateway

27. _____ is used for hiding the payment information from the merchant and order information from payment authority.

(A) SET.

(B) SSL.

(C) HTTP.

(D) PGP.

28. Which process will ensure that the issues of the credit card is an approved transactions ?

(A) Payment capture

(B) Payment authorization

(C) Purchase request

(D) Purchase reply

29. IPsec is designed to provide security at the _____.

(A) Transport layer

(B) Network layer

(C) Application layer

(D) Session layer

30. IPsec protects the _____, in tunnel mode.

(A) Entire IP packet

(B) IP header

(C) IP payload

(D) IP trailer

31. 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

32. An attempt to make a computer resource unavailable to its intended users is called_____.

(A) Denial-of-service attack

(B) Virus attack

(C) Worms attack

(D) Botnet process

33. Which one of the following is not a higher-layer SSL protocol ?

(A) Alert Protocol

(B) Handshake Protocol

(C) Alarm Protocol

(D) Change Cipher Spec Protocol

34. The full form of SSL is :

(A) Serial Session Layer

(B) Secure Socket Layer

(C) Session Secure Layer

(D) Series Socket Layer

35. Which protocol consists of only 1 bit ?

(A) Alert protocol

(B) Handshake protocol

(C) Upper-Layer protocol

(D) Change Cipher Spec protocol

36. Which protocol is used for the purpose of copying the pending state into the current state ?

(A) Alert protocol

(B) Handshake protocol

(C) Upper-Layer protocol

(D) Change Cipher Spec protocol

37. Which of the following usually observe each activity on the internet of the victim, gather all information in the background and send it to someone else ?

(A) Malware

(B) Spyware

(C) Adware

(D) All of the above

38. It can be a software program or a hardware device that filters all data packets coming through the internet, a network etc. it is known as the _____.

(A) Antivirus

(B) Firewall

(C) Cookies

(D) Malware

39. Can it be possible that in some cases, hacking a computer or network can be legal ?

(A) No, in any situation, hacking can be legal

(B) It may be possible that in some cases, it can be referred to as a legal task

(C) Can't be said

(D) Never

40. Which of the following refers to the violation of the principle, if a computer is no more accessible ?

(A) Access control

(B) Confidentiality

(C) Availability

(D) All of the above

41. Which one of the following refers to the technique used for verifying the integrity of the message ?

(A) Digital signature

(B) Decryption algorithm

(C) Protocol

(D) Message Digest

42. In system hacking, which of the following is the most crucial activity ?

(A) Information gathering

(B) Covering tracks

(C) Cracking passwords

(D) None of the above

43. To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.

(A) Antivirus

(B) Firewall

(C) Vlc player

(D) Script

44. Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system ?

(A) DDos and DOS

(B) Malware & Malvertising

(C) Phishing and Password attacks

(D) All of the above

45. Hackers usually used the computer virus for _____ purpose.

(A) To log, monitor each and every user's stroke

(B) To gain access the sensitive information like user's Id and Passwords

(C) To corrupt the user's data stored in the computer system

(D) All of the above

46. Which of the following statements is correct about the firewall ?

(A) It is a device installed at the boundary of a company to prevent unauthorized physical access

(B) It is a device installed at the boundary of an incorporate to protect it against the unauthorized access

(C) It is a kind of wall built to prevent files form damaging the corporate.

(D) None of the above

47. Which one of the following statements is correct about Email security in the network security methods ?

(A) One has to deploy hardware, software and security procedures to lock those apps down

(B) One should know about what the normal behavior of a network look likes so that he/she can spot any changes, breaches in the behavior of the network

(C) Phishing is one of the most commonly used methods that are used by hackers to gain access to the network

(D) All of the above

48. Which of the following statements is true about the VPN in Network security ?

(A) It helps to ensure that communication between a device and a network is secure

(B) It is usually based on the IPsec (IP Security) or SSL (Secure Sockets Layer)

(C) It typically creates a secure, encrypted virtual "tunnel" over the open internet

(D) All of the above

49. Which of the following type of text is transformed with the help of a cipher algorithm ?

(A) Transformed text

(B) Complex text

(C) Scalar text

(D) Plain text

50. Which type of the following Malware does not replicate or clone them self's through infection ?

(A) Rootkits

(B) Trojans

(C) Worms

(D) Viruses

51. Which of the following statements is true about the Trojans ?

(A) Trojans perform tasks for which they are designed or programmed, need host program

(B) Trojans, need host program, replicates them self's or clone them self's through an infections

(C) Trojans do nothing harmful to the user's computer systems

(D) Trojans replicate

52. Which of the following is a type of independent malicious program that never required any host program ?

(A) Trojan Horse

(B) Worm

(C) Trap Door

(D) Virus

53. Name of RSA algorithm is based on :

(A) Name of the mathematicians who proposed it

(B) Name of the technique

(C) Resource secure algorithm

(D) Revises secure algorithm

54. DNS translates a Domain name into _____.

(A) Hex

(B) Binary

(C) IP

(D) URL

55. SNMP means :

(A) Secure network management process

(B) Strong network management protocol

(C) Simple network management protocol

(D) Simple network management process

56. The application-level protocol in which a few manager stations control a set of agents in called _____.

(A) HTML

(B) TCP

(C) SNMP

(D) SNMP/IP

57. The main difference between SNMPv3 and SNMPv2 is _____.

(A) Management

(B) Integration

(C) Classification

(D) Enhanced security

58. SNMP is the framework for managing devices in an internet using the _____.

(A) TCP/IP protocol

(B) UDP

(C) SMTP

(D) None

59. A manager is a host that runs a SNMP _____ process.

(A) Client

(B) Server

(C) Both (A) and (B)

(D) None of the above

60. An agent is a host or computer that runs a SNMP _____ process.

(A) Client

(B) Server

(C) Both (A) and (B)

(D) None of the above

61. Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN ?

(A) AH transport mode

(B) ESP transport mode

(C) ESP tunnel mode

(D) AH tunnel mode

62. Which type(s) of encryption protocol(s) can be used to secure the authentication of computers using IPsec ?

(A) Kerberos version 5

(B) SHA

(C) MD5

(D) Both SHA and MD5

63. Which provides authentication at the IP level ?

(A) AH

(B) ESP

(C) PGP

(D) SSL

64. IPsec defines two protocols :_____ and _____.

(A) AH, SSL

(B) PGP, SMIME

(C) AH, ESP

(D) PGP, ESP

65. Public key encryption/decryption is not preferred for confidentiality of message because :

(A) It is slow

(B) It is hardware/software intensive

(C) It has a high computational load

(D) All of the mentioned

66. Which one of the following is not a for public key distribution ?

(A) Public-Key Certificates

(B) Hashing Certificates

(C) Publicly available directories

(D) Public-Key authority

67. What is the PGP stand for ?

(A) Permuted Gap Permission

(B) Permuted Great Privacy

(C) Pretty Good Permission

(D) None of the mentioned

68. Which of the following public key distribution systems is most secure ?

(A) Public-Key Certificates

(B) Public announcements

(C) Publicly available directories

(D) Public-Key authority

69. Which system uses a trusted third party interface ?

(A) Public-Key Certificates

(B) Public announcements

(C) Publicly available directories

(D) Public-Key authority

70. Which of the following is not an element/field of the X.509 certificates ?

(A) Issuer Name

(B) Serial Modifier

(C) Issuer unique identifier

(D) Signature

71. Playfair cipher is an example of _____.

(A) Mono-alphabetic cipher

(B) Poly-alphabetic cipher

(C) Transposition cipher

(D) Additive cipher

72. Rail fence cipher is an example of _____.

(A) Mono-alphabetic cipher

(B) Substitution cipher

(C) Transposition cipher

(D) Additive cipher

73. Which of the following ciphers are created by shuffling the letters of a word ?

(A) Substitution cipher

(B) Transposition cipher

(C) RSA cipher

(D) DSS cipher

74. Which of the following is are two types of traditional cipher ?

(A) Transposition cipher and replacement cipher

(B) Transposition cipher and substitution cipher

(C) Transforming cipher and substitution cipher

(D) Transforming cipher and replacement cipher

75. In which of the following cipher the plain text and the ciphered text have same letters ?

(A) Autokey cipher

(B) Rail fence cipher

(C) Vigenere cipher

(D) Additive cipher

76. DES follows :

(A) Hash Algorithm

(B) Caesars Cipher

(C) Feistel Cipher Structure

(D) SP Networks

77. The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key.

(A) 12

(B) 18

(C) 9

(D) 16

78. In the DES algorithm the round key is _____ bits.

(A) 48

(B) 64

(C) 56

(D) 32

79. In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q' ?

(A) p and q should be divisible by $\Phi(n)$

(B) p and q should be co-prime

(C) p and q should be prime

(D) p/q should give no remainder

80. In RSA, $\Phi(n)$ = _____ in terms of p and q.

(A) (p)/(q)

(B) (p)(q)

(C) (p-1)(q-1)

(D) (p+1)(q+1)

81. Dual signature is a concept used in :

(A) PGP

(B) IPSEC

(C) IPSEC

(D) SET

82. Key management in IPSEC uses :

(A) Oakley key mgmt. protocol, Deffie hellman

(B) ISAKMP, Oakley key mgmt. protocol

(C) Deffie hellman

(D) DSS

83. Message authentication code, a cryptographic scheme is used for which security service ?

(A) Authentication

(B) Integrity

(C) Key exchange

(D) Confidentiality

84. SET is used for :

(A) Payment by debit card for online purchase

(B) Payment by credit card for online purchase

(C) Payment by any card

(D) None of the above

85. X.509 uses the basic concept of :

(A) Digital signature

(B) Encryption

(C) Public key certificate

(D) Compression

86. Which is not an entity of SET ?

(A) Acquirer

(B) Issuer

(C) Payment gateway

(D) Payment authorization

87. Which of the following combination is symmetric cipher ?

(A) DES, RSA, DIFFIE HELLMAN

(B) MD5, SHA1, DSS

(C) IDEA, CAST, 3 DES

(D) DSS, RC4, IDEA

88. Conventional encryption and public keyencryption are also called _____ and _____ respectively.

(A) Asymmetric encryption, symmetric encryption

(B) Symmetric encryption, one key encryption

(C) Symmetric encryption, asymmetric encryption

(D) None of the above

89. Masquerade is a/an :

(A) Active attack

(B) Passive attack

(C) Cryptanalysis

(D) None of the above

90. Which is harmful effect of virus ?
(A) Damage file, slows down the system
(B) Increasing efficiency
(C) Decreasing file size
(D) None of the above

91. A computer program that copies itself to other computer across the internet is known as :
(A) Virus
(B) Trojan horse
(C) Worm
(D) Bot

92. Nonce in Cryptography :
(A) Is used to verify fraudulent digital signature
(B) Is used in authentication protocol to defend against replay attack
(C) Used to check the integrity of message
(D) All of the above

93. The process through which an illegitimate website pretends to be a specific legitimate site is known as :
(A) Snigffing
(B) Snoofing
(C) Backdoor
(D) Intrusion detection

94. Network layer firewall works as a _____.
(A) Frame filter
(B) Application gateway
(C) Content filter
(D) Packet filter

95. 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) VSPN
(C) VAN
(D) VPN

96. Which of the following is a disadvantage of Circuit-level gateway firewalls ?
    (A) They're expensive
    (B) They're complex in architecture
    (C) They're complex to setup
    (D) They do not filter individual packets
97. Which of the following about VPNs is correct ?
    (A) Always more expensive than leased lines
    (B) Always cheaper than leased lines
    (C) Usually more expensive than leased lines
    (D) Usually cheaper than leased lines
98. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____.
    (A) Barrier point
    (B) Chock point
    (C) Firewall point
    (D) Gatekeeper point
99. A proxy firewall filters at _____.
    (A) Application layer
    (B) Data link layer
    (C) Network layer
    (D) Transport layer
100. Packet filtering firewalls are vulnerable to _____.
    (A) Inrusion
    (B) MiTM
    (C) Phishing
    (D) Spoofing

******

DO NOT OPEN THE QUESTION BOOKLET UNTIL ASKED TO DO SO

1. Examinee should enter his / her roll number, subject and Question Booklet Series correctly in the O.M.R. sheet, the examinee will be responsible for the error he / she has made.
2. **This Question Booklet contains 100 questions, out of which only 75 Question are to be Answered by the examinee. Every question has 4 options and only one of them is correct. The answer which seems correct to you, darken that option number in your Answer Booklet (O.M.R ANSWER SHEET) completely with black or blue ball point pen. If any examinee will mark more than one answer of a particular question, then the answer will be marked as wrong.**
3. Every question has same marks. Every question you attempt correctly, marks will be given according to that.
4. Every answer should be marked only on Answer Booklet **(O.M.R ANSWER SHEET).**Answer marked anywhere else other than the determined place will not be considered valid.
5. Please read all the instructions carefully before attempting anything on Answer Booklet**(O.M.R ANSWER SHEET).**
6. After completion of examination, please hand over the **O.M.R. SHEET** to the Examiner before leaving the examination room.
7. There is no negative marking.

Note: On opening the question booklet, first check that all the pages of the question booklet are printed properly in case there is an issue please ask the examiner to change the booklet of same series and get another one.