Online Examinations (Even Sem/Part-I/Part-II Examinations 2020 - 2021

Course Name - –Cryptography
Course Code - MSCME409

* You can submit the form ONLY ONCE.
* Fill the following information for further process.

* Required

1. Email *

2. Name of the Student *

3. Enter Full Student Code *

4. Enter Roll No *

5. Enter Registration No *

6. Enter Course Code *

7. Enter Course Name *

8. *

Mark only one oval.

- Diploma in Pharmacy
- Bachelor of Pharmacy
- B.TECH.(CSE)
- B.TECH.(ECE)
- BCA
- B.SC.(CS)
- B.SC.(BT)
- B.SC.(ANCS)
- B.SC.(HN)
- B.Sc.(MM)
- B.A.(MW)
- BBA
- B.COM
- B.A.(JMC)
- BBA(HM)
- BBA(LLB)
- B.OPTOMETRY
- B.SC.(MB)
- B.SC.(MLT)
- B.SC.(MRIT)
- B.SC.(PA)
- LLB
- B.SC(IT)-AI
- B.SC.(MSJ)
- Bachelor of Physiotherapy
- B.SC.(AM)
- Dip.CSE
- Dip.ECE
- DIP.EE
- DIP.CE

- DIP.ME
- PGDHM
- MBA
- M.SC.(BT)
- M.TECH(CSE)
- LLM
- M.A.(JMC)
- M.A.(ENG)
- M.SC.(MATH)
- M.SC.(MB)
- MCA
- M.SC.(MSJ)
- M.SC.(AM)
- M.SC.CS)
- M.SC.(ANCS)
- M.SC.(MM)
- B.A.(Eng)

Answer all the questions. Each question carry one mark.

9. 1. The remainder when the sum 4!+5!+6!+....+50! is divided by 4 is

Mark only one oval.

- 1
- 2
- 3
- 0

10. 2. ___ is an inverse of 11 modulo 12

Mark only one oval.

- 1
- 2
- 5
- 0

11. 3. The _____ is the original message before transformation.

Mark only one oval.

- ciphertext
- plaintext
- secret-text
- None of these

12. 4. A(n) _____ algorithm transforms plaintext to ciphertext

Mark only one oval.

- encryption
- decryption
- Either encryption or decryption
- Neither encryption nor decryption

13. 5. A combination of an encryption algorithm and a decryption algorithm is called a _____

Mark only one oval.

- cipher
- secret
- key
- none of these

14. 6. In a(n) _____ cipher, the same key is used by the sender and the receiver.

Mark only one oval.

- symmetric-key
- asymmetric-key
- either symmetric-key or asymmetric-key
- neither symmetric-key nor asymmetric-key

15. 7. In a(n) _____ cipher, a pair of keys is used.

Mark only one oval.

- symmetric-key
- asymmetric-key
- either symmetric-key or asymmetric-key
- neither symmetric-key nor asymmetric-key

16. 8. In an asymmetric-key cipher, the receiver uses the _____ key.

Mark only one oval.

- private
- public
- either private or public
- neither private nor public

17. 9. _____ cipher can be categorized into two broad categories: monoalphabetic and polyalphabetic.

Mark only one oval.

- substitution
- transportation
- either substitution or transportation
- neither substitution nor transportation

18. 10. The Caesar cipher is a _____ cipher that has a key of 3.

Mark only one oval.

- transportation
- additive
- shift
- none of these

19. 11. A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.

Mark only one oval.

- S-box
- P-box
- T-box
- None of these

20. 12. A modern cipher is usually a complex _____ cipher made of a combination of different simple cipher.

Mark only one oval.

- round
- circle
- square
- None of these

21. 13. DES is a(n) _____ method adopted by the U.S. government.

Mark only one oval.

- symmetric key
- asymmetric key
- either symmetric key or asymmetric key
- neither symmetric key nor asymmetric key

22. 14. DES has an initial and final permutation block and _____ rounds.

Mark only one oval.

- 14
- 15
- 16
- None of these

23. 15. DES uses a key generator to generate sixteen _____ round keys.

Mark only one oval.

- 32-bit
- 48-bit
- 54-bit
- 42-bit

24. 16. _____ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data.

Mark only one oval.

- AEE
- AED
- AER
- AES

25. 17. ECB and CBC are _____ ciphers.

Mark only one oval.

- block
- stream
- field
- None of these

26. 18. The _____ method provides a one-time session key for two parties.

Mark only one oval.

- Diffie-Hellman
- RSA
- DES
- AES

27. 19. An asymmetric-key (or public-key) cipher uses

Mark only one oval.

- 1 key
- 2 key
- 3 key
- 4 key

28. 20. We use Cryptography term to transforming messages to make them secure and immune to _____

Mark only one oval.

- change
- idle
- attacks
- defend

29. 21. In asymmetric-key cryptography, the two keys, e and d, have a special relationship to _____

Mark only one oval.

- others
- data
- key
- each other

30. 22. The substitutional ciphers are _____

Mark only one oval.

- monoalphabetic
- semialphabetic
- polyalphabetic
- both monoalphabetic and polyalphabetic

31. 23. DES stand for

Mark only one oval.

- Data Encryption Standard
- Data Encryption Subscription
- Data Encryption Solutions
- Data Encryption Slots

32. 24. A substitution cipher replaces one symbol with _____

Mark only one oval.

- same symbol
- provide two symbols for each
- another
- all of these

33. 25. In Cryptography, the original message, before being transformed, is called _____

Mark only one oval.

- simple text
- plain text
- empty text
- filled text

34. 26. For RSA to work, the value of m must be less than the value of

Mark only one oval.

- p
- q
- n
- r

35. 27. The original message, before being transformed, is _____

Mark only one oval.

- cipher text
- plain text
- decryption
- none of these

36. 28. Data Encryption Standard (DES) was designed by

Mark only one oval.

- Intel
- IBM
- HP
- Sony

37. 29. In asymmetric-key cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is _____

Mark only one oval.

- short
- long
- flat
- thin

38. 30. The ciphers of today are called

Mark only one oval.

- substitution cipher
- round cipher
- transposition cipher
- none of these

39. 31. In symmetric-key cryptography, the same key is used by _____

Mark only one oval.

- one party
- multi party
- third party
- both party

40. 32. If the plain text is CAESAR and the shift cipher text is FDHVDU, then the key is

Mark only one oval.

- 1
- 2
- 3
- 4

41. 33. An encryption scheme in which each letter of the original message is replaced by the same cipher substitute is known as a _____

Mark only one oval.

- monoalphabetic cipher
- polyalphabetic cipher
- monoalphabetic cipher & polyalphabetic cipher
- none of these

42. 34. The numerical version of READY modulo 26 is

Mark only one oval.

- 17 04 00 03 24
- 16 04 00 03 24
- 17 03 00 03 24
- 17 04 00 03 23

43. 35. The set of plaintexts is always

Mark only one oval.

- finite
- infinite
- may be finite or infinite
- null

44. 36. The receiver is named as

Mark only one oval.

- Alice
- Bob
- Oscar
- none of these

45. 37. In cryptography, what is cipher?

Mark only one oval.

- algorithm for performing encryption and decryption
- encrypted message
- both algorithm for performing encryption and decryption and encrypted message
- decrypted message

46. 38. Which one of the following algorithm is not used in asymmetric-key cryptography?

Mark only one oval.

- rsa algorithm
- diffie-hellman algorithm
- electronic code book algorithm
- dsa algorithm

47. 39. What is data encryption standard (DES)?

Mark only one oval.

- block cipher
- stream cipher
- bit cipher
- byte cipher

48. 40. Which one of the following is a cryptographic protocol used to secure HTTP connection?

Mark only one oval.

- stream control transmission protocol (SCTP)
- transport layer security (TLS)
- explicit congestion notification (ECN)
- resource reservation protocol

49. 41.ElGamal encryption system is _____

Mark only one oval.

- symmetric key encryption algorithm
- asymmetric key encryption algorithm
- not an encryption algorithm
- block cipher method

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

Mark only one oval.

- fixed size bit string
- variable size bit string
- both fixed size bit string and variable size bit string
- variable sized byte string

51. 43. Which of the following is not a type of symmetric-key cryptography technique?

Mark only one oval.

- Caesar cipher
- Data Encryption Standard (DES)
- Diffie Hellman cipher
- Playfair cipher

52. 44. Which of the following security attacks is not an active attack?

Mark only one oval.

- Masquerade
- Modification of message
- Denial of service
- Traffic analysis

53. 45. "A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?

Mark only one oval.

- An integer values
- A square matrix
- An array of characters (i.e. a string)
- All of these

54. 46. To encrypt the plaintext, a cryptographic algorithm works in combination with a key _____

Mark only one oval.

- Word, number, or phrase
- Special Symbols
- Function Keys
- All of these

55. 47. The Data Encryption Standard (DES) is an example of a _____

Mark only one oval.

- Conventional cryptosystem
- Asymmetric cryptosystem
- Caesar's cryptosystem
- All of these

56. 48. Security Goals of Cryptography are _____

Mark only one oval.

- Confidentiality
- Authenticity
- Data integrity
- All of these

57. 49. The private key in asymmetric key cryptography is kept by

Mark only one oval.

- Sender
- Receiver
- Sender and receiver
- All the connected devices to the network

58. 50. The keys used in cryptography are

Mark only one oval.

- secret key
- Private key
- Public key
- All of them

59. 51. Symmetric-key cryptography started thousands of years ago when people needed to exchange

Mark only one oval.

- files
- packets
- secrets
- transmission

60. 52. Cryptography, a word with Greek origins, means

Mark only one oval.

- Corrupting Data
- Secret Writing
- Open Writing
- Closed Writing

61. 53. The Advanced Encryption Standard (AES) was designed

Mark only one oval.

- National Institute of Standards and Technology
- IBM
- HP
- Intel

62. 54. In Cryptography, when text is treated at the bit level, each character is replaced by

Mark only one oval.

- 4 Bits
- 6 Bits
- 8 Bits
- 10 Bits

63. 55. This is an encryption/decryption key known only to the party or parties that exchange secret messages.

Mark only one oval.

- e-signature
- digital certificate
- private key
- security token

64. 56. Today, many Internet businesses and users take advantage of cryptography based on this approach.

Mark only one oval.

- public key infrastructure
- output feedback
- Encrypting File System
- single signon

65. 57. Developed by Philip R. Zimmermann, this is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

Mark only one oval.

- DSS
- OCSP
- Secure HTTP
- Pretty Good Privacy

66. 58. This is the encryption algorithm that will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years as the new standard encryption algorithm.

Mark only one oval.

- Rijndael
- Kerberos
- Blowfish
- IPsec

67. 59. This is the inclusion of a secret message in otherwise unencrypted text or images.

Mark only one oval.

- masquerade
- steganography
- spoof
- eye-in-hand system

68. 60. This is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding ciphertext value and vice versa.

Mark only one oval.

- footprinting
- hash function
- watermark
- Electronic Code Book