VI Semester B.C.A. Degree Examination, September/October 2022
(CBCS) (F+R)
COMPUTER SCIENCE
BCA 603T : Cryptography and Network Security

Time : 3 Hours

Max. Marks : 100

Instruction : *Answer all Sections.*

SECTION – A

I. Answer **any ten** questions. **Each** question carries **2** marks.   **(10×2=20)**

   1) What is Cryptography ?
   2) Define encryption and decryption.
   3) What is Coprime ? Give an example.
   4) Differentiate between monoalphabetic and polyalphabetic cipher.
   5) What is Rail Fence Cipher ? Give an example.
   6) Define Digital Signature.
   7) What are the protocol's used to provide IP Security ?
   8) What is payload ?
   9) What is a session ?
   10) What is IPSec ?
   11) Write any two applications of RSA Algorithm.
   12) What is Trapdoor one way function ?

SECTION – B

II. Answer **any five** questions. **Each** question carries **five** marks.   **(5×5=25)**

   13) Explain various security services.
   14) Explain Extended Euclidean algorithm with an example.
   15) Write short notes on Ceaser cipher with example.
   16) Difference between Symmetric and Asymmetric Key.
   17) Write short notes on A5/1 stream cipher.
   18) Explain square root test for prime number.
   19) Write short notes on Internet Key Exchange.
   20) Explain X.509 certificate.

P.T.O.

SECTION – C

III. Answer any three questions. Each question carries fifteen marks.   (3×15=45)

21) a) Explain various cryptographic attacks.   8
    b) Explain Single Linear Congruence equation with an example.   7

22) a) Explain Playfair Cipher with an example.   8
    b) Explain Data Encryption Standard function.   7

23) a) Explain RSA Cryptosystem.   8
    b) Explain Fermat primality test with an example.   7

24) a) Explain Diffie Hellman Key Exchange with example.   8
    b) Write short notes on Kerberos.   7

25) a) Explain IPSec two modes.   7
    b) Explain Transport layer security and their protocol.   8

SECTION – D

IV. Answer any one question. Each question carries 10 marks.   (1×10=10)

26) Explain the solution for Chinese Remainder theorem.   10

$x \equiv 2(mod3)$

$x \equiv 3(mod5)$

$x \equiv 2(mod7)$

27) Explain briefly Advanced Encryption standard with neat diagram.   10

_____

VI Semester B.C.A. Examination, September/October 2022
(CBCS) (F + R) (2016 – 17 and Onwards)
COMPUTER SCIENCE
BCA 603 : Cryptography and Network Security

Time : 3 Hours

Max. Marks : 100

Instruction : *Answer **all** the Sections.*

SECTION – A

Answer **any ten** questions. **Each** question carries **two** marks. (10×2=20)

1. Name any two active attacks.

2. Define monoalphabetic cipher.

3. Define block cipher.

4. Differentiate steganography and water marking.

5. What is Avalanche effect ?

6. What is residue class ?

7. Define trapdoor one-way function.

8. Write any two attacks on RSA.

9. What is Kerberos ?

10. Define S/MIME.

11. What is blind signature ?

12. List two protocols which provide security for emails.

SECTION – B

Answer **any five** questions. **Each** question carries **five** marks. (5×5=25)

13. Explain various security mechanisms. 5

14. Explain play fair cipher with an example. 5

15. What is cryptographic hash function ? Explain its properties. 5

P.T.O.

16. Write a note on steganography.   5

17. Compare AES and DES.   5

18. Explain Fermat's little theorem.   5

19. What is PKI ? What are main duties of PKI ?   5

20. Explain the two modes of operation in IPSec.   5

SECTION – C

Answer **any three** questions. Each question carries **fifteen** marks.   (3×15=45)

21. a) Explain any three types of cryptoanalytic attacks.   8

    b) Explain extended Euclidean algorithm with an example.   7

22. a) Explain the four stages of AES algorithm.   8

    b) Explain multiple DES.   7

23. a) Explain any two probabilistic algorithms for primality testing.   8

    b) State and explain Chinese Remainder theorem with an example.   7

24. a) Explain Whirlpool Cipher.   8

    b) Explain X.509 certificate.   7

25. a) Explain the protocols in SSL.   8

    b) Write a note on IKE.   7

SECTION – D

Answer **any one** question. **Each** question carries **ten** marks.   (1×10=10)

26. Explain RSA cryptosystem.   10

27. Explain security policy inbound and outbound processing.   10

VI Semester B.C.A. Degree Examination, September/October 2022
(CBCS – Freshers and Repeaters)
COMPUTER SCIENCE
Paper – BCA 602T : System Programming

Time : 3 Hours

Max. Marks : 100

Instruction : *Answer all Sections.*

SECTION – A

Answer **any ten** of the following. **Each** question carries **2** marks. (10×2=20)

1. What is Application Software ?

2. List the advantages of using base register.

3. What is location counter ? What its purpose ?

4. List any two advantages assembly language.

5. Differentiate DC and DS.

6. Differentiate between a macro and subroutine.

7. What is macro call ?

8. Mention the functions of loader.

9. What is MDT and MNT ?

10. What is a token ? Give example.

11. What is a symbol table ? Give its format.

12. Define local and global optimization.

SECTION – B

Answer **any five** questions. **Each** question carries **5** marks. (5×5=25)

13. Explain open subroutine and closed subroutine with an example.

14. Explain the general machine structure with neat diagram.

15. Sort the following numbers using interchange sort technique :
9, 6, 2, 12, 11, 9, 3, 7.

P.T.O.

16. Explain formal system.

17. Explain pass 2 overview of an assembler with flowchart.

18. Explain macro definition with arguments with an example.

19. Explain different types of cards used in direct linking loader.

20. Discuss briefly about lexical phase of compiler.

SECTION – C

Answer any three questions. Each question carries **15** marks.   (3×15=45)

21. a) Explain various instruction formats used in IBM-360.   8

    b) Explain time sharing operating system.   7

22. a) Give format of all five tables used in assembler.   8

    b) Draw the detailed pass-1 flowchart of an assembler.   7

23. a) Explain ALA, MDT, MNT format with an example.   8

    b) Explain conditional macro expansion.   7

24. a) Explain design of absolute loader with a neat diagram.   8

    b) Explain compile and go loader with a neat diagram.   7

25. a) Explain the structure of a compiler with a neat diagram.   8

    b) Explain syntax phase of a compiler.   7

SECTION – D

Answer **any one** question. **Each** question carries **10** marks.   (1×10=10)

26. a) Draw micro-flowchart for ADD instruction.   5

    b) Explain any five pseudo-ops used in assembly language program.   5

27. a) Explain :   5
    i) Micro language
    ii) Macroprocessor

    b) List the databases used by pass-1 and pass-2 of a macroprocessor.   5

VI Semester B.C.A. Examination, September/October 2022
(CBCS) (F + R) (2016 – 17 and Onwards)
COMPUTER SCIENCE
BCA – 602 : System Programming

Time : 3 Hours

Max. Marks : 100

Instruction : *Answer all the Sections.*

SECTION – A

I. Answer **any ten** questions, **each** carries **two** marks.   (2×10=20)

1) Define system software and application software.

2) List the components of system software.

3) What is program counter ?

4) Write the syntax of USING and DROP.

5) What is sorting ? Give example.

6) Write format of MOT table.

7) Give two difference between macros and subroutine.

8) Define macros and give its syntax.

9) What are the functions of loader ?

10) What is dynamic loading ?

11) What is a token ? Give example.

12) Define local and global optimization.

SECTION – B

II. Answer **any five** questions, **each** carries **five** marks.   (5×5=25)

13) Explain the general machine structure of IBM 360 machine with a neat diagram.

14) Explain overview flowchart for pass1 of an assembler.

15) Explain macro instruction with arguments with an example.

16) Explain compile and go loader with a diagram.

P.T.O.

7

17) Explain machine dependent optimization of a compiler.

18) Explain micro flowchart for ADD instruction.

19) Explain four types of cards used in direct linking loader.

20) Sort the following elements using address calculation sort.

19, 13, 11, 5, 26, 1, 16, 9, 27, 2.

SECTION – C

III. Answer **any three** questions, **each** carries **fifteen** marks.   (3×15=45)

21) a) Explain different instruction formats of IBM 360/370 machine.   8
    b) Explain any five pseudo-op with an example.   7

22) a) Explain in detail pass 2 algorithm of an assembler.   8
    b) Explain binary search with an example.   7

23) a) Explain implementation of a macro processor.   8
    b) Explain the database formats of MDT, MNT and ALA of a macro processor.   7

24) a) Explain the design of an absolute loader with a neat diagram.   8
    b) Give the specification of databases used in pass 1 and pass 2 of direct linking loader with a neat diagram.   7

25) a) Explain the structure of a compiler with a neat diagram.   10
    b) Explain syntax phase of a compiler.   5

SECTION – D

IV. Answer **any one** question, **each** carries **ten** marks.   (1×10=10)

26) a) Give the purpose of pass 1 and pass 2 of an assembler.   5
    b) Draw the block diagram of general loading scheme and explain.   5

27) a) Explain macro definition, macro call and macro expansion with example.   5
    b) Explain open subroutine and closed subroutine with an example.   5

_____

96052

Version Code

A

Question Booklet Sl. No.

NA108357

INSTRUCTIONS TO CANDIDATES

1. Immediately after the commencement of the Examination, you should check that this Booklet does not have any unprinted or torn or missing pages or items, etc. If any of the above defects is found, get it replaced by a Complete Question Booklet of the available series.

2. Write clearly the Question Booklet Version Code **A**, **B**, **C** or **D** in the appropriate space provided for the purpose, in the OMR Answer Sheet.

3. Enter the name of the Subject, Reg. No., Student ID, Q.P. Code, Question Booklet version code and affix Signature on the OMR sheet. As the answer sheets are designed to suit the Optical Mark Reader (OMR) system, special care should be taken to fill those items accurately.

4. This Question Booklet contains **55** questions, **Part – A** contains **40** questions of **one** mark each. **Part – B** contains **15** questions of **two** marks **each**. **All** questions must be attempted. Each question contains four answers, among them one correct answer should be selected and shade the corresponding option in the OMR sheet.

5. All the answers should be marked only on the OMR sheet provided and only with a **black** or **blue** ink ball point pen. If more than one circle is shaded / wrongly shaded / half shaded for a given question no marks will be awarded.

6. Immediately after the final bell indicating the closure of the examination, stop making any further markings in the OMR Answer Sheet. Be seated till the OMR Answer Sheet is collected. After handing over the OMR Answer Sheet to the Invigilator you may leave the examination hall.

PART – A

(40×1=40)

Answer all the questions. Each question carries **1** mark.

1. A database management system DBMS is
   A) Collection of interrelated data
   B) Collection of programs to access data
   C) Collection of data describing one particular enterprise
   D) All of the above

2. Which of the following is not a database user ?
   A) Database administrator
   B) Windows user
   C) Database designer
   D) End user

3. DDL stands for
   A) Dynamic Data Language
   B) Detailed Data Language
   C) Data Definition Language
   D) Data Derivation Language

4. MS word is
   A) Database
   B) Presentation package
   C) Spreadsheet
   D) Word processor

SPACE FOR ROUGH WORK

A

5. What is the default font used in MS Word ?

A) Times New Roman

B) Calibri

C) Arial

D) Preeti

6. Drop cap means

A) All caps

B) Small caps

C) Title case

D) None of the above

7. An Excel workbook is a collection of

A) Workbooks

B) Worksheets

C) Charts

D) Worksheet and charts

8. How many worksheets can a workbook have ?

A) 3

B) 8

C) 255

D) None of the above

SPACE FOR ROUGH WORK

A

9. Which symbol must all formula begin with ?

A) =

B) +

C) (

D) @

10. This key uniquely identifies each record

A) Primary key

B) Key record

C) Unique key

D) Field name

11. What are the columns in a Microsoft Access table called ?

A) Rows

B) Records

C) Fields

D) Columns

12. Which of the following store comment to retrieve data from database ?

A) Forms

B) Reports

C) Queries

D) Tables

SPACE FOR ROUGH WORK

A

13. Microsoft PowerPoint is a

A) Database

B) Spreadsheet

C) Presentation Package

D) Word processing

14. Which is the view used to deliver your presentation to audience ?

A) Slide view

B) Normal view

C) Slide show view

D) Slide sorter view

15. Which of the following section does not exist in a slide layout ?

A) Titles

B) Lists

C) Charts

D) Animations

16. URL stands for

A) Universal Resource Locator

B) Uniform Resource Locator

C) Uniform Radio Locator

D) None of these

SPACE FOR ROUGH WORK

A

13

17. Which one of the following is not a search engine ?

   A) Bing

   B) Google

   C) Yahoo

   D) Windows

18. Verification of a login name and password is known as

   A) Configuration

   B) Accessibility

   C) Authentication

   D) Logging in

19. When you delete the file the file goes to ?

   A) Recycle bin

   B) Control panel

   C) My computer

   D) Windows

20. Information system consist of

   A) Software

   B) Hardware

   C) People

   D) All of the above

SPACE FOR ROUGH WORK

A

21. The backbone of any organization is

   A) Information

   B) Employee

   C) Management

   D) Capital

22. Any organized system for the collection, organization, storage and communication of information is known as

   A) Computer System

   B) Internet System

   C) Information System

   D) All of the above

23. ERP stands for

   A) Enterprise Resource Programming

   B) Enterprise Resource Planning

   C) Enterprise Resource Production

   D) Enterprise Resource Purchase

24. Which system is used to support decision makers ?

   A) MRP

   B) DSS

   C) KDD

   D) SCM

SPACE FOR ROUGH WORK

A

25. ISO stands for

    A) International Student Organization

    B) International Service Organization

    C) International Security Organization

    D) International Standard Organization

26. The international cyber security standard is

    A) ISO 27001

    B) ISO 27002

    C) ISO 27003

    D) ISO 27004

27. Which of the following is a cyber crime ?

    A) Hacking

    B) Worm attack

    C) Virus attack

    D) All of these

28. ERM stands for

    A) Enterprise Risk Management

    B) Environment Risk Management

    C) Establishment Risk Management

    D) Electronic Risk Management

SPACE FOR ROUGH WORK

A

29. How many levels of CMM stages refer to an organizations process management capabilities ?

    A) 2   B) 3

    C) 4   D) 5

30. The components of COBIT are

    A) Framework

    B) Process descriptions

    C) Maturity models

    D) All the above

31. A common way through which commercial contracts can be entered electronically

    A) Email

    B) Website

    C) Google

    D) None of the above

32. Digital signature is

    A) Scanned signature on computer

    B) Code number of the sender

    C) Public key encryption

    D) Software to recognize signature

SPACE FOR ROUGH WORK

A

33. _____ a security method in which information is encoded in such a way that only authorized user can read it.

A) Private key

B) Public key

C) Encryption

D) Decryption

34. Unencrypted data is called

A) Ciphertext

B) Plaintext

C) Hypertext

D) None of the above

35. Which is the type of electronic fund transfer ?

A) NEFT

B) RTGS

C) IMPS

D) All the above

36. E-Banking also known as

A) Internet banking

B) Online banking

C) Virtual banking

D) All the above

SPACE FOR ROUGH WORK

A

37. The card which you cannot buy a product is

    A) Credit card

    B) ATM card

    C) Debit card

    D) Smart card

38. Information Technology (Amendment) Act, 2008 as come into force in

    A) January 2008

    B) October 2009

    C) October 2008

    D) January 2009

39. Verification of electronic record is possible through

    A) Public key

    B) Private key

    C) Digital signature

    D) E-governance

40. Digital signatures created and verified using

    A) Program

    B) Graphical coding

    C) HTML

    D) Cryptography

SPACE FOR ROUGH WORK

PART – B

Answer **all** the questions. **Each** question carries **2** marks :

(15×2=30)

41. The key which is not selected primary key is known as

   A) Super key

   B) Candidate key

   C) Secondary key

   D) Composite key

42. An advantage of the database management approach is

   A) Data is independent on programs

   B) Data redundancy increases

   C) Data is integrated and can be accessed by multiple programs

   D) None of the above

43. Ctrl + F is used for

   A) Open find and replace dialogue box with activating find tab

   B) Open page setup dialogue box with activating layout tab

   C) Open font dialogue box with activating font tab

   D) Open file save as dialogue box

SPACE FOR ROUGH WORK

A

44. The function used to find average of list of cells

A) Avg()

B) Average()

C) Total()

D) Sum()

45. Which of the following is the latest version of Excel ?

A) Excel 2000

B) Excel 2002

C) Excel ME

D) Excel XP

46. The most popular commercial DBMS is

A) Microsoft SQL server

B) Microsoft access

C) My SQL

D) Oracle

47. What is the maximum zoom percentage in Microsoft PowerPoint ?

A) 100

B) 200

C) 300

D) 400

SPACE FOR ROUGH WORK

A

96052

48. MIME stands for

    A) Multipurpose Internet Mail Extensions

    B) Multipurpose Internet Mail Email

    C) Multipurpose Internet Mail End

    D) Multipurpose Internet Main Extra

49. Which is domain of artificial intelligence ?

    A) Virtual reality

    B) Intelligent agents

    C) Expert system

    D) All the above

50. ERP use software application to _____ the processes of an organization

    A) Automate

    B) Speed

    C) Growth

    D) None of the above

51. The criminal activities carried out by means of computers are the internet is

    A) Computer intrusion

    B) Social engineering

    C) Cyber crime

    D) Masquerading

_____

SPACE FOR ROUGH WORK

A

52. COBIT stands for

A) Current Objectives For Information And Related Technology

B) Capable Objectives For Information And Related Technology

C) Control Objectives For Information And Related Technology

D) Common Objectives For Information And Related Technology

53. E-Commerce means

A) Email Commerce

B) Electric Commerce

C) Electronic Commerce

D) Electro Commerce

54. The authentication to be affected by use of asymmetric crypto system and hash function is known as

A) Public key

B) Private key

C) Digital signature

D) E-governance

55. Which is The Act which provides legal framework for e-governance in India ?

A) IT Act, 2000

B) Indian Penal Code

C) IT (Amendment) Act, 2008

D) None of the above

SPACE FOR ROUGH WORK

A

65624

VI Semester B.C.A. Degree Examination, September/October 2022
(CBCS) (F+R)
COMPUTER SCIENCE
B.C.A. 604T : Web Programming

Time : 3 Hours

Max. Marks : 70

Instruction : Answer all Sections.

SECTION – A

I. Answer any ten questions. Each question carries **2** marks. (10×2=20)

1) What is IP Address ? Give an example.

2) List the HTTP Request Methods.

3) What are the three types of XHTML DOC Types ?

4) Differentiate Absolute and Relative URL.

5) Give any two advantages of CSS.

6) List the properties of CSS.

7) What are the data types available in javascript ?

8) List the windows objects.

9) What is a Namespace ?

10) What is object constructor ?

11) Mention any four features of XML.

12) What is a schema ?

SECTION – B

II. Answer **any five** questions. **Each** question carries **10** marks. (5×10=50)

13) a) Explain image tag with a suitable example.

   b) How a link is created within a page ? Give an example. (5+5)

14) a) Explain row spanning and Col. spanning in table creation with an example.

   b) Describe any five HTTP methods. (5+5)

P.T.O.

15) a) Explain different types of selectors in CSS.

    b) Explain CSS Box model.   **(5+5)**

16) a) List and explain any five math objects.

    b) Explain the input and output methods in Javascript.   **(5+5)**

17) a) Describe the looping statements with suitable example.

    b) Explain all pattern matching methods in Javascript.   **(5+5)**

18) a) Explain event and event handling in Javascript.

    b) List and explain all the events in XHTML.   **(5+5)**

19) a) Define DTD. Explain internal and external DTD.

    b) What is meant by absolute positioning ? How it is used in webpage creation ?   **(5+5)**

20) a) Explain XML Processor.

    b) Explain XML Schema.   **(5+5)**

UG – 423

VI Semester B.C.A. Examination, Sept./Oct. 2022
(CBCS) (F+R) (2016-17 and Onwards)
COMPUTER SCIENCE
BCA 604 : Web Programming

Time : 3 Hours

Max. Marks : 70

Instruction : Answer all the Sections.

SECTION – A

I. Answer any ten questions. Each question carries two marks.　　(2×10=20)

1) What is IP address ?

2) Define HTML.

3) What is MIME ?

4) Write any two empty elements in HTML.

5) What is the use of anchor tag in HTML ?

6) Define JavaScript.

7) What is the use of <DIV> tag ?

8) What do you mean by the absolute positioning of an element ?

9) What is the use of event handler ?

10) Define <img> tag.

11) Write any two differences between HTML and XML.

12) What are mouse events ?

SECTION – B

II. Answer any five questions. **Each** question carries **ten** marks.　　(5×10=50)

13) a) Define web server. Explain Apache and IIS web servers.　　5

   b) Write the applications of Internet.　　5

14) a) Explain the ordered list in HTML with example.　　5

   b) Write the tags used to create the table.　　5

P.T.O.

15) a) Write the different levels of CSS with example. 6

    b) Explain the get and post request methods. 4

16) a) Explain any 3 selectors in CSS with example. 6

    b) Explain the attributes of input tag with example. 4

17) a) Write the data types used in JavaScript with example. 5

    b) Write a JavaScript program to find the biggest of three numbers. 5

18) Explain FORM components with example. 10

19) a) Define DTD. Explain external DTD and internal DTD. 5

    b) Write any five XHTML tags with examples. 5

20) a) Explain DOM with example. 5

    b) Write in detail about XML. 5

_____