Roll No. ..... Total Pages : 4

BCA–303

B.C.A. (Third Year) Examination, 2019

INFORMATION SECURITY AND CRYPTOGRAPHY

Paper–III

Time Allowed : Three Hours

Maximum Marks : 100

PART–A [Marks : 20

Answer all questions (50 words each).

All questions carry equal marks.

PART–B [Marks : 50

Answer **five** questions (250 words each), selecting **one** question from each Unit. All questions carry equal marks.

PART–C [Marks : 30

Answer any **two** questions (300 words each).

All questions carry equal marks.

Scanned with CamScanner

PART–A

1. Answer the following questions : 10×2=20

(i) What is mean by Cryptography ?

(ii) Define the Public Key.

(iii) What is mean by Pseudorandom bits ?

(iv) What is basic objective of Software based generator ?

(v) Define the Data Encryption.

(vi) What is mean by Vigenere Ciphers ?

(vii) Define the Authentication.

(viii) What is Kerberos ?

(ix) Define the Digital signature.

(x) What is a Protocol ?

PART–B

UNIT–I

2. Discuss the block Cipher and Stream Cipher Encryption mechanism. 10

3. Explain the key management through Symmetric key and Public Key techniques. 10

Scanned with CamScanner

UNIT–II

4. Discuss the stream Ciphers based on LFSRS and its property. 10

5. Write short notes on the following :

   (a) Test for measuring Randomness.

   (b) Blum-Blum-Shub Pseudorandom bit generator. 5,5

UNIT–III

6. Discuss the modes of operation of block Ciphers. 10

7. Explain RSA algorithm with examples. 10

UNIT–IV

8. Explain MDS and Secure hash algorithm (SHAI). 10

9. What is mean by user Authentication ? Discuss the Biometric Authentication. 10

UNIT–V

10. Discuss the techniques for distributing public keys and make a comparison between them. 10

Scanned with CamScanner

(3) 2019

11. What is meant by Digital signature ? Discuss the classification of Digital signature schemes. 10

PART–C

12. Write short notes on the following :

    (a) Symmetric Key v/s Public Key Cryptography.

    (b) Models for evaluating security. 8,7

13. (a) Properties of Synchronous and Self Synchronizing Stream Cipher.

    (b) Hardware based and Software based generator. 7,8

14. Discuss Data encryption standard algorithm and Knapsack encryption algorithm. 15

15. Write short notes on the following :

    (a) Comparison between Different message digest algorithm.

    (b) Certificate based Algorithm. 10,5

16. Discuss the techniques for distributing confidential key and key management life cycle. 15

Scanned with CamScanner