This question paper contains 4 printed pages]

BCA-303

B.C.A. (Third Year) EXAMINATION, 2018

Paper III

(Information Security and Cryptography)

Time allowed : Three Hours

Maximum Marks : 100

Part A (खण्ड 'अ') [Marks : 20]

*Answer all questions (**50** words each).*

***All** questions carry equal marks.*

***सभी** प्रश्न अनिवार्य हैं । प्रत्येक प्रश्न का उत्तर **50** शब्दों से अधिक न हो । **सभी** प्रश्नों के अंक समान हैं ।*

Part B (खण्ड 'ब') [Marks : 50]

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

***All** questions carry equal marks.*

*प्रत्येक इकाई से **एक** प्रश्न चुनते हुए, कुल **पाँच** प्रश्न कीजिए । प्रत्येक प्रश्न का उत्तर **250** शब्दों से अधिक न हो । **सभी** प्रश्नों के अंक समान हैं ।*

Part C (खण्ड 'स') [Marks : 30]

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

***All** questions carry equal marks.*

*कोई **दो** प्रश्न कीजिए । प्रत्येक प्रश्न का उत्तर **300** शब्दों से अधिक न हो । **सभी** प्रश्नों के अंक समान हैं ।*

P.T.O.

Part A

1. Answer the following questions :

   (*i*) What do you mean by Cryptography ?

   (*ii*) Why do we need of security ?

   (*iii*) Name the tests for measuring randomness.

   (*iv*) What are the properties of self-synchronizing stream cipher ?

   (*v*) What do you mean by Multiple encryption ?

   (*vi*) IDEA stands for ?

   (*vii*) Name some popular techniques of user authentication.

   (*viii*) What is message digest ?

   (*ix*) What is Digital signature ?

   (*x*) What is importance of key management in cryptography ?

Part B

Unit I

2. Explain basic terminology and goals of cryptography.

3. What are attacks on encryption scheme ? Also explain models for evaluating security.

Unit II

4. Explain Random bit generation techniques in detail.

5. Explain stream cipher in detail.

Unit III

6. Explain all block cipher modes.

7. Explain knapsack encryption algorithm by taking suitable example.

Unit IV

8. What do you mean by message authentication ? Explain message digest in detail.

9. Explain kerberos and certificate based authentication technique.

Unit V

10. Explain various attacks on signature.

11. What are the techniques for distributing public key ?

Part C

12. Explain Symmetric key *V/s* Public key cryptography.

13. Explain Blum-Blum-Shub pseudorandom bit generator.

14. Explain IDEA in detail.

15. Explain MDS algorithm.

16. Explain key management life-cycle.