

Roll No.....

Total No. of Printed Pages : 4

BCA-303

B.C.A. Third Year Examination, 2017

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** from each Unit. All questions carry equal marks.

प्रत्येक इकाई में से एक-एक प्रश्न चुनते हुए, कुल पाँच प्रश्न कीजिए। प्रत्येक प्रश्न का उत्तर 250 शब्दों से अधिक न हो।

सभी प्रश्नों के अंक समान हैं।

BCA-303/AG/1890/78

P. T. O.

PART-C (खण्ड-स) [Marks : 30

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

All questions carry equal marks.

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

PART-A

1. Answer the following questions :

- (i) What is Plain text and Cipher text?
- (ii) What is Block Cipher?
- (iii) What is Random bit generation?
- (iv) Explain SEAL in short?
- (v) Differentiate between CFB and OFB mode?
- (vi) What is Symmetric key cryptography?
- (vii) What is Message Digest?
- (viii) What is Kerberos?
- (ix) What is Key management?
- (x) What is Digital envelop?

PART-B

UNIT-I

2. Explain the basic concepts of Cryptography?
3. Explain Key Management through Symmetric Key and Public key techniques?

UNIT-II

4. Explain various tests for measuring Randomness in brief?
5. Explain Properties of LFSRs based stream cipher?

UNIT-III

6. Explain Data encryption standard algorithm.
7. Explain RSA algorithm by taking suitable example.

UNIT-IV

8. Explain about MD5 algorithm in detail.
9. Explain Single Sign On (SSO) approach.

UNIT-V

10. Explain various attacks on signature.
11. What are the techniques for distributing confidential key?

PART-C

12. Why we need of Security? Explain security approaches. Also explain models for evaluating security.
13. Discuss various properties of Linear and Non-linear feedback shift registers.
14. Explain knapsack encryption algorithm?
15. Explain various user authentication techniques in detail.
16. Write a short note on Key Management Techniques.
