

Roll No.....

2

BCA-601(N)

B.C.A. (Semester-VI) Examination -2014

(New Course)

Paper: First

Computer Network Security

Time: Three Hours]

[Maximum Marks: 75

Note: Section A is compulsory. Attempt seven questions from Section B and one question from Section C.

Section-A

1. (a) What is a Transposition Cipher? Illustrate with an example? (4)
- (b) What do you understand by Network Security Attack? Describe active and passive security attacks. (4)

Section-B

2. Explain Feistel Encryption and Decryption algorithm. What is the difference between confusion and diffusion? (8)

BCA-601(N)-H-1850

3. What is Triple DES? Explain the term meet-in-middle attack. (8)
4. What is the difference between stream and block ciphers? (8)
5. Define a group with its properties. (8)
6. What is ring? Also explain its properties. (8)
7. List three classes of polynomial arithmetic. (8)
8. Describe and illustrate Chinese Remainder theorem (8)
9. Given that 2 is primitive root of 19 Determine all other primitive root. (8)
10. Write the different uses of public-key cryptography. (8)

BCA-601(N)-H-1850

Section- C

1. Write and explain Diffie-Hellman key exchange. (11)

Or

2. What are different security issues of RSA? (11)

<http://csjmuonline.com>

Whatsapp @ 9300930012

Your old paper & get 10/-

पुराने पेपर्स भेजे और 10 रुपये पायें,

Paytm or Google Pay से