Roll No. .....

BCA–601(N)

B. C. A. (Sixth Semester)
EXAMINATION, May/June, 2015

(New Course)

Paper First

COMPUTER NETWORK SECURITY

Time : Three Hours] [*Maximum Marks : 75*

Note : Attempt questions from all Sections as directed.

Section—A 3 each

(Short Answer Type Questions)

Note : All questions are compulsory.

1. (A) Define the following terms :

   (i) Authentication

   (ii) Data Confidentiality

   (iii) Access control

   (B) Write in short about different types of possible passive attacks.

   (C) What do you understand by the term Denial of Service ?

   (D) What are the primitive roots of 19 ?

(E) Draw and write in short about simplified model of conventional encryption.

(F) What is the difference between block cipher and stream cipher ?

(G) List the properties of modulo operator.

(H) Write down the *four* different stages used by AES.

(I) What are the notes of Public and Private keys ? Explain.

Section—B 12 each

(Long Answer Type Questions)

Note : Attempt any *two* questions.

2. Discuss any *two* substitution techniques used for encryption using examples.
3. Using diagram discuss the S-DES key generation method.
4. What is a random number ? How do you generate cryptographically secure pseudonumber ?
5. (a) Explain avalanche effect.

   (b) What do you mean when you say "b is a divisor of a" ? Explain with an example.

Section—C 8 each

(Long Answer Type Questions)

Note : Attempt any *two* questions.

6. What is a key distribution center ? List the ways in which secret key can be distributed. Differentiate between session and master keys.

7. Perform encryption and decryption using RSA algorithm given :

$$p = 3, q = 11, e = 7, m = 5$$

What do you understand by digital signature ?

8. Write in short about Fermat's and Euler's theorems.
9. What are the principal elements of a public key crypto-system ? Explain.