Roll No. .....

BCA–602

# B. C. A. (Sixth Semester) EXAMINATION, 2010

Paper Second

## NETWORK SECURITY

*Time : Three Hours* ] [ *Maximum Marks : 70*

**Note :** Attempt any *five* questions. All questions carry equal marks.

1. (a) What are the various security goals ? Explain.

   (b) Prove, using mod operator, that the remainder of any integer when divided by 100 is the integer made of the two right most digits.

2. (a) Describe five security services. Also give the examples.

   (b) We have been told that the remainder of an integer divided by 5 is the same as the remainder of division of the rightmost digit by 5. Use the properties of the mod operator to prove this claim.

3. (a) Define various security mechanisms employed in cryptography.

   (b) Encrypt and then decrypt the message "The dark horse will certainly win the race" using the keyed columnar transposition cipher.

P. T. O.

- - - 17 - 249

4. (a) Compare and contrast attacks on digital signature with attacks on cryptosystems.

   (b) Define the RSA digital signatures scheme and compare it to the RSA cyptosystem.

5. (a) What is Linear Diophantine equation of two variables ? How many solution such an equation have ? Show that there are no solutions to the following Linear Diophantine equations :

   (i) $15x + 12y = 13$

   (ii) $18x + 30y = 20$

   (b) Define Kerberos X-509 and name its servers. Briefly explain the duties of each server.

6. (a) Distinguish between a substitution cipher and a transposition cipher.

   (b) A customer wants to cash Rs. 500 and get some Rs. 50 and Rs. 30 bills. Find various valid combinations.

7. (a) Elaborate S/Mine Security architecture.

   (b) What is DES function ? Why does the DES function need an expansion permutation ?

8. Explain the following (any *four*) :

   (i) Electronic mail security

   (ii) Message digest algorithm

   (iii) Euler's theorem

   (iv) Block cipher modes of operation

   (v) Hill cipher

   (vi) One time pad



250