(Following Paper ID and Roll No. to be filled in your Answer Book)

**PAPER ID : 214406** Roll No | | | | | | | | | | |

# MCA

## (SEM. IV) THEORY EXAMINATION 2013-14

## NETWORK SECURITY AND CRYPTOGRAPHY

*Time : 3 Hours* *Total Marks : 100*

**Note :**–Attempt **all** questions.

### SECTION–A

1. Attempt **all** parts : **(2×10=20)**

(a) How many keys are required for two people to communicate via a cipher ?

(b) What are the two general approaches to attacking a cipher ?

(c) Distinguish between differential and linear cryptanalysis.

(d) What is the key size for Blowfish ?

(e) What is a key distribution center ?

(f) Describe in general terms an efficient procedure for picking a prime number.

(g) Name the four key steps in the creation of a digital certificate.

(h) What are the three aspects of a 3-factors authentication ?

(i) What four requirements were defined for Kerberos ?

(j) What is the purpose of the SSL alert protocol ?

## SECTION–B

2. Attempt any **three** parts of this Section : **(10×3=30)**

(a) What is encryption ? What is decryption ? Draw a block diagram showing plaintext, cipher text, encryption and decryption.

(b) Demonstrate that Blowfish decryption is the inverse of Blowfish encryption.

(c) Describe RSA algorithm. Suppose in a public key stream using RSA, the two prime numbers are p = 17 and q = 31. The public key is e = 7. Determine the private key. Perform the encryption and decryption of message m = 2.

(d) Describe the Digital Signature Algorithm (DSA) of digital signature standard.

(e) What services are provided by IPSec ? Explain the transport and tunnel modes of IPSec.

## SECTION–C

**Note:**– Attempt **all** questions in this Section. **(10×5=50)**

3. Attempt any **two** part of the following : **(5×2=10)**

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

(b) Why do some block cipher modes of operation only use encryption while others use both encryption and decryption ?

(c) Distinguish between symmetric and asymmetric key cryptography.

4. Attempt any **two** parts of the following : **(5×2=10)**

(a) How can the same key be reused in triple DES ?

(b) What is triple encryption ?

(c) Describe the Man-in-the-middle attack on double DES.

5. Attempt any **two** parts of the following : **(5×2=10)**

(a) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography.

(b) State and prove Euler's theorem.

(c) Write the steps of RSA key generation

6. Attempt any **two** parts of the following : **(5×2=10)**

(a) What are some approaches to producing message authentication ?

(b) What are the properties a digital signature should have ?

(c) What is the difference between a message authentication code and one-way hash function ?

7. Attempt any **two** parts of the following : **(5×2=10)**

(a) Why is the SSL layer positioned between the application layer and the transport layer ?

(b) What are the limitations of a firewall ?

(c) What can be the two main attacks on corporate networks ?