8. (a) What is the use of NAT ? How does it takes place ? Illustrate with example. **9**

(b) Identify two web based applications for which SSL is appropriate and two applications for which it is not appropriate. In each case explain clearly why is it appropriate or why it is not ? **6**

No. of Printed Pages : 04 **Roll No. .....**

DD-687

M.C.A. EXAMINATION, May 2017

(Fourth Semester)

(B. Scheme) (Main & Re-appear)

NETWORK SECURITY AND MANAGEMENT

MCA-556

Time : 3 *Hours*] [*Maximum Marks :* 75

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit. All questions carry equal marks.

Unit I

1. (a) Explain the components of symmetric and asymmetric encryption system. **9**

(b) List three advantages and three disadvantages of stream ciphers. **6**

2. (a) What is access control ? How is it different from availability ? **5**

(b) Write and discuss any *five* principles of network security. **10**

Unit II

3. Differentiate between : **15**

(a) Authentication and authorization

(b) Password based authentication and two factor authentication

(c) Digital Signatures and digital certificates.

4. Consider the field, F(19) and Elliptic Curve, $y^2 = x^3 + 3x^2 + 1$ over F(19).

(i) List all the points on this curve

(ii) Compute –(17, 14)

(iii) Compute (8, 9) + (12, 13)

(iv) Compute 2 X (17, 14)

(v) Use the double and add technique to compute 13 X (11,14).

Unit III

5. Describe the operation of any *two* speech scramblers. **15**

6. Differentiate between :

(i) Narrow band and wide band systems for speech encryption **7.5**

(ii) Analog and digital systems for speech encryption. **7.5**

Unit IV

7. (a) What is the use of digital certificate ? Explain the meaning of all the fields of X.509 digital certificate format. **2,6**

(b) Explain, how cryptographic hash is used to provide message authentication and message integrity. **7**