TY BSc IT / 78

Q.P. Code : 23202

(Time: $2\frac{1}{2}$ hours)

Total Marks: 75

N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt *any two* of the following: **10**

a. Explain different principles of security.

b. List and explain different types of criminal attacks. Give example of each one.

c. List different transposition techniques. Explain any one with example.

d. A and B want to establish a secrete key using the Diffie-Hellman Kay Exchange protocol. Assuming the values as n=11,g=5,x=2 and y=3, find out the values of A,B and the secret key.

2. Attempt *any two* of the following: **10**

a. Explain cipher feedback mode.

b. Explain DES algorithm.

c. How subkey is generated for rounds of IDEA algorithm?

d. Explain the working of RC5.

3. Attempt *any two* of the following: **10**

a. Explain with example RSA algorithm.

b. Write down difference between symmetric and asymmetric key cryptography.

c. Explain how MD5 works.

d. What is message authentication code? Write down disadvantages of hash-based message authentication code.

4. Attempt *any two* of the following: **10**

a. List and explain various fields in a X.509 digital certificate version 3.

b. What is need of self-signed digital certificates and cross certificate?

c. Write down the difference between online certificate revocation status checks and simple certificate validation protocol.

d. List and explain PKIX services.

5. Attempt *any two* of the following: **10**

a. Explain the purchase request transaction of SET.

b. List different email security protocols. Explain any one in detail.

c. Explain IP Datagram format.

d. List and explain different fields of security association database.

[TURN OVER]

Q.P. Code : 23202

6. Attempt *any two* of the following: **10**

a. What is authentication token? Explain how it works. Also list different types of authentication token.

b. What is the use of smart cards? Write down the problems and their solutions related to smart card technology.

c. Write a short note on Kerberos.

d. Write a short note on one-way authentication.

7. Attempt *any three* of the following: **15**

a. List and explain different types of attacks.

b. Explain how subkey is generated in blowfish algorithm.

c. Write down difference between MD5 and SHA-1.

d. List different public key cryptography standards. Explain any two of them.

e. What is electronic money? Classify electronic money based on
   i. Tracking of money
   ii. Involvement of the bank in the transaction.

f. List and explain different approaches to achieve SSO.
