TyIT / **Paper / Subject Code: 53601 / Network Security** / 7

(2½ 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. Describe the terms IP sniffing, IP spoofing.
   b. What are the general types of attacks?
   c. What are the key principles of security? Explain.
   d. What is virus? What are its lifetime phases?

2. **Attempt *any two* of the following:** 10
   a. Illustrate the sub-key generation process of each round of Blow Fish.
   b. What is the concept of chaining in cipher block chaining (CBC) mode? Explain.
   c. Explain the concept of International Data Encryption Algorithm (IDEA).
   d. Write a short note on Data Encryption Standard (DES).

3. **Attempt *any two* of the following:** 10
   a. What is the real crux of RSA? Explain.
   b. Describe the advantages & disadvantages of Symmetric & Asymmetric key cryptography.
   c. Write a short note on hash based message authentication code (HMAC).
   d. What is the concept of message digest? Explain.

4. **Attempt *any two* of the following:** 10
   a. List & explain the services of the PKIX model.
   b. What are the technical contents of the digital certificate? Explain.
   c. Explain Kerberos.
   d. What are the types of digital certificates? Explain.

5. **Attempt *any two* of the following:** 10
   a. Explain Multipurpose Internet Mail Extensions (MIME).
   b. Write a short note on Application gateway.
   c. Outline the broad level steps of SET.
   d. Explain Transmission Control Protocol (TCP) segment header format in detail.

6. **Attempt *any two* of the following:** 10
   a. What is the significance of the authentication with clear text password? What are the problems with clear text passwords? Explain.
   b. What is single sign-on systems (SSO) approach? Explain.
   c. Explain the concept of Authentication Token.
   d. Write a note on Biometric Authentication.

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

a. What is the difference between passive attack and active attack?

b. Explain the block cipher technique.

c. Define message digest. What are the key requirements of message digest? Explain.

d. Name & explain the 4 steps on the creation of the digital certificate.

e. How does PGP works? Explain.

f. List the security handshake Pitfalls & explain any one of them.
