TYIT (II) /NS/75

April – 2018

Q.P. Code :01760

[Time: $2\frac{1}{2}$ Hours] [Marks:75]

Please check whether you have got the right question paper.

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.

Q.1 **Attempt any two of the following:** (10)

a. Explain Phishing and Pharming attacks in detail.
b. Explain the principles of security.
c. List and explain types of criminal attracts.
d. Explain Hill cipher with example.

Q.2 **Attempt any two of the following:** (10)

a. List all the algorithm modes in cryptography. Explain any two in detail.
b. How DES works? Explain.
c. Explain in detail one round in IDEA.
d. What are the features of blowfish algorithm? Explain the steps in encryption process using blowfish algorithm.

Q.3 **Attempt any two of the following:** (10)

a. Compare symmetric and asymmetric key cryptography using their various characteristics.
b. How Hash-based Message authentication works? Explain.
c. Explain the concept of Digital Envelope.
d. How RSA can be used in digital signature? Explain in detail.

Q.4 **Attempt any two of the following:** (10)

a. What are the typical contents of a digital certificate?
b. Describe the role of CA in creation / revocation of Digital Certificate.
c. What is cross certification? Why is needed?
d. Draw and explain the format of CRL.

Q.5 **Attempt any two of the following:** (10)

a. List phases of SSL handshake. Explain any two phases in detail.
b. Draw and explain SET model.
c. Write a note on VPN.
d. Explain different firewall configurations.

Q.6 **Attempt any two of the following:** (10)

a. What is authentication token? Explain its working.
b. Explain how Challenge / Response tokens works.
c. Explain the password based authentication and the problems associated with it.
d. Write a note on single sign on approaches.

Q.7 **Attempt any three of the following:** (15)

a. Explain Diffie Hellman Key exchange algorithm with example
b. Explain processes in each round of AES.
c. Explain the working of SHA (Secure Hash Algorithm).
d. Explain PKS# 14 Pseudo-random Number Generation Standard.
e. Explain PGP operations.
f. Write a detailed note on biometric authentication.