T.Y. B.Sc. (IT) : Sem. V

Network Security

Prelim Question Paper

Time : 2½ Hrs.] **[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 questions** 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 the following (any **TWO**) **[10]**
(a) Explain CIA security goals.
(b) Describe Diffie-Hellman Key Exchange Algorithm.
(c) What is the principle behind Vernam Cipher (OTP)? Why is it highly secure? Explain with an example.
(d) List and explain different types of criminal attacks.

2. Attempt the following (any **TWO**) **[10]**
(a) Describe CFB (Cipher Feed Back) Mode in detail.
(b) List all 5 steps of DES round and explain Key Transformation and X-OR and Swap steps in detail.
(c) Explain the principles/working of IDEA algorithm.
(d) Write a short note on RC4.

3. Attempt the following (any **TWO**) **[10]**
(a) Explain the security solution based on the concept of Digital Envelope/Key Wrapping
(b) List and explain RSA algorithm steps with an example.
(c) List and explain requirements of message Digest.
(d) Describe the Problems with Public Key Exchange.

4. Attempt the following (any **TWO**) **[10]**
(a) Explain PKCS#5 PBE – Password Based Encryption Standard.
(b) Explain the Station to Station Protocol.
(c) List and explain the types or categories of Digital Certificates
(d) Write a short note on CRL –Offline Revocation Status Check.

5. Attempt the following (any **TWO**) **[10]**
(a) Describe Packet Filters.
(b) Write a short on VPN (Virtual Private Network).
(c) Write a short note on PGP (Pretty Good Privacy)
(d) Explain the SET Process.

6. Attempt the following (any **TWO**) **[10]**
(a) Explain the working of Kerberos Protocol.
(b) What are One-Way Authentication approaches? Explain any two.
(c) Explain ClearText(Plain text) password based authentication and problems associated with it.
(d) Describe various Biometrics Techniques

P.T.O.

7. Attempt the following (any **THREE**) **[15]**

(a) Encrypt the message 'Come Home Tomorrow using : Caeasar Cipher and Simple Columnar transposition techniques with 4 columns and its order is 4,2,1,3.

(b) Write a short note on BlowFish Algorithm.

(c) Explain HMAC in detail.

(d) Explain the steps in creation of Digital Certificate

(e) Describe the Handshake Protocol of SSL.

(f) Write a short note on Authentication Token and explain any one type in detail.

Paper Discussion Schedule for all Subjects

Date	Day	Timing	Centre
5 Nov.2016	Saturday	9.00 a.m. to 11.00 a.m.	Ghatkopar
5 Nov.2016	Saturday	12.00 p.m. to 2.00 p.m.	Thane
5 Nov.2016	Saturday	3.00 p.m. to 5.00 p.m.	Dombivli
6 Nov.2016	Sunday	9.00 a.m. to 11.00 a.m.	Dadar
6 Nov.2016	Sunday	12.00 p.m. to 2.00 p.m.	Andheri
6 Nov.2016	Sunday	3.00 p.m. to 5.00 p.m.	Borivali
7 Nov.2016	Monday	9.00 a.m. to 11.00 a.m.	Nerul

❑ ❑ ❑ ❑ ❑