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. Answer any **TWO** of the following: **[10]**
(a) Explain with example different approaches to implement security model.
(b) Encrypt the message 'Come Home Tomorrow' using
(i) Ceaser Cipher
(ii) Simple Columner Transposition Techniques with four columns. Order is 3, 2, 4, 1
(c) Explain how attackers misuse cookies to collect important information.
(d) List possibilities of attacks when the sender of a message encrypts the plain text message into its corresponding cipher text.

2. Answer any **TWO** of the following : **[10]**
(a) List different types of cryptography algorithms. Explain with example.
(b) Explain the steps in various rounds of AES.
(c) Explain subkey generation process of blowfish algorithm.
(d) Explain double DES algorithm.

3. Answer any **TWO** of the following: **[10]**
(a) How is RSA is used in digital signatures? Explain.
(b) Explain the working of secure hash algorithm-512.
(c) Explain the working of HMAC.
(d) Explain Elipitic Curve Cryptography and EIGamal.

4. Answer any **TWO** of the following: **[10]**
(a) Describe of the various fields of X.509v3 digital certificate.
(b) How is digital certificate is verified? Explain.
(c) Why do we trust digital certificate?
(d) List and explain public key cryptograph standards.

5. Answer any **TWO** of the following: **[10]**
(a) Explain the handshake protocol.
(b) Explain the Secure Electronic Transaction process.
(c) With neat diagram write the internal operaitons of 3-D secure protocol.
(d) List the different firewall configuraitons. Explain any two.

6. Answer any **TWO** of the following: **[10]**
(a) How does clear text password work? What are the problems with it?
(b) Write a short note on key distribution center.
(c) Explain the working of how challenge/response tokens.
(d) What are the One-way authenticaiton approaches? Explain any two.

7. Attempt any **THREE** of the following : **[15]**
   (a) Write a short note on phishing.
   (b) Explain subkey generaiton process of each round of international data encryption algorithm.
   (c) Explain with a neat diagram the man-in-middle attack.
   (d) Why is a self-signed certificate needed?
   (e) Explain the working of how pretty good privacy.
   (f) How does certificate-based authentication work? Explain.

Paper Discussion Schedule for all Subjects

Date	Day	Timing	Centre
23 Oct. 2017	Monday	5.00 p.m. to 7.00 p.m.	Nerul
24 Oct. 2017	Tuesday	9.00 a.m. to 11.00 a.m.	Ghatkopar
24 Oct. 2017	Tuesday	12.00 p.m. to 2.00 p.m.	Thane
24 Oct. 2017	Tuesday	3.00 p.m. to 5.00 p.m.	Dombivli
25 Oct. 2017	Wednesday	9.00 a.m. to 11.00 a.m.	Dadar
25 Oct. 2017	Wednesday	12.00 p.m. to 2.00 p.m.	Andheri
25 Oct. 2017	Wednesday	3.00 p.m. to 5.00 p.m.	Borivali

❑ ❑ ❑ ❑ ❑