Roll No. .....

Total Pages : 3

218302

May, 2019

M.TECH CSE - 3rd Semester

Network Security (MCSE-17-203)

Time : 3 Hours] [Max. Marks : 75

Instructions :

1. *It is compulsory to answer all the questions (1.5 marks each) of Part-A in short.*
2. *Answer any four questions from Part-B in detail.*
3. *Different sub-parts of a question are to be attempted adjacent to each other.*

PART–A

1. (a) Which technique (cryptography or stegnography) is used in the case when :

A student writes the answer to a test on small piece of paper, rolls up the paper, rolls up the paper, and insert it in a ball-point pen, and passes the pen to the another student. (1.5)

(b) Write an example of replay attack which leads to masqurade attacks? (1.5)

(c) Differentiate between confusion and diffusion? (1.5)

(d) Some archeologists found a new script written in an unknown language. The archeologists later found a small tablet at the same place that contains a sentence in the same language with the translation in Greek. Using the tablet, they were able to read the original script. What type of attack did the archeologists use? (1.5)

(e) Why does the 64 bit DES function need an expansion permutation? (1.5)

(f) In RSA : Given p = 1, q = 23, and e = 3 find n, ?(n), and d. (1.5)

(g) Differentiate between Trojan and worm? (1.5)

(h) What is the Significance of Authentication server in Kerberos? (1.5)

(i) List out various fields of X.509 certification for version 3? (1.5)

(j) What is Security Parameter Index (SPI)? (1.5)

PART–B

2. (a) Explain in detail various aspects of information security? (10)

(b) Discuss Triple DES with three keys and Triple DES with two keys? (5)

3. (a) Explain Man in the Middle Attack in diffie-hellman algorithm? (5)

(b) Give some scenarios where SSL protocol can provide security? Explain various security parameters and protocols used by SSL for providing security? (10)

4. What is the major differences of issues in IP security protocols used at network layer and SSL/TLS protocols used at transport protocols? How these protocols are different from the Security protocols used at application layers? (15)

5. (a) Differentiate between Spoofing and Snooping? (5)

(b) How can Kerberos protocol be helpful to provide entity authentication? Explain in detail various steps used for this purpose? (10)

6. (a) Explain in detail AES algorithm with the help of an example. (7.5)

(b) Explain in detail Secure Hyper Text transfer protocol in detail. (7.5)

7. Write short note on :

(a) Secure Electronic Transaction (SET).

(b) Types of firewalls. (15)