Roll No. .... IT Total Pages : 3

203601

MAY, 2019
B.Tech. VI SEMESTER
Network Security (IT-302-C)

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) Distinguish among vulnerability, threat and control. (1.5)

(b) Differentiate between confusion and diffusion. (1.5)

(c) Encrypt the following message using mono-alphabetic substitution cipher with key = 5.

Plain-Text is : "**I am a Hacker**". (1.5)

(d) What are Computer criminals? (1.5)

(e) Perform Rail-Fence Transposition technique on the following message

Plain-Text is : "**Happy Birthday to you**". (1.5)

(f) How a circuit gateway is different from an application gateway firewall. (1.5)

(g) What is the purpose of S-box in DES? (1.5)

(h) Describe Authentication Header. (1.5)

(i) Discuss Distributed Denial of Service Attack. (1.5)

(j) Cite a reason why an organization might want two or more firewalls on a single network. (1.5)

PART–B

2. (a) Consider a program to accept and tabulate votes in an election. Who might want to attack the program? What types of harm might they want to cause? What kind of vulnerabilities might they exploit to cause harm? (5)

(b) Alice meets the Bob and says **Rjjy rj ts ymj xfggfym.bj bnqq inxhzxx ymj uqfs.** If she is using Caesar Cipher, What does she want to convey? (10)

3. (a) Differentiate between AES and DES. Explain DES and its implementation. (10)

(b) Discuss Kerberos Protocol. What is the Kerberos protocol used for? What entities are involved in the Kerberos protocol? What assumptions need to be in place before use of the Kerberos protocol? (5)

4. (a) Explain different types of malicious codes or intruders. Also discuss Virus and its related threats. (10)

(b) Explain MD5 Algorithm. (5)

5. (a) What is Play fair Cipher? Suppose keyword is **'PLAY FAIR EXAMPLE'** and the Plain-text is **'MY NAME IS ATUL'**.

Convert this Plain text into Cipher text using Play fair Cipher Technique. (10)

(b) How IPSec provides security? Would you consider IPSec as a replacement for SSL. (5)

6. (a) Why SSL layer is positioned between the application layer and transport layer? Explain the purpose of the SSL Alert Protocol. (10)

(b) Explain PGP. What is the concept of Key rings in PGP? (5)

7. What are the types of analysis adopted by intrusion detection and protection System (IDPS)? What are the types of IDPS? (15)