5

Sr. No. 003704

Dec 2021

B.Tech(CE/CSE) VII SEMESTER

Cryptography and Network Security (PEC-CS-A-703)

Time: 90 Minutes **Max. Marks:25**

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

PART -A

Q1 (a) Discuss the goals of computer security. (1)

(b) Transform using Rail-fence Technique. (1)
Plain Text= **Happy Birthday to You.**

(c) Differentiate between vulnerability and threat. (1)

(d) Why some attacks are called passive? Why are other attacks passive? (1)

(e) List three applications where stream ciphers are desirable? (1)

(f) Encrypt using Playfair Cipher. (1)
Plain Text=**My Name is Atul**. Key=**Harsh**

(g) What are Byzantine attacks in MANET. (1)

(h) Describe Sinkhole attacks. (1)

(i) What is e-mail security? (1)

(j) Describe the security challenges in WSN. (1)

PART -B

Q2 (a) Why do encryption key should be changed from time to time? How frequently should a cryptographic key be changed? Explain with the help of an example. (3)

(b) Explain x.509 authentication service. (2)

Q3 (a) Describe Polyalphabetic substitution cipher with an example. Explain cryptoanalysis of Polyalphabetic ciphers. (3)

(b) Explain Diffie-Hellman Key Exchange Algorithm. (2)

Q4 What is IP sec protocol? Explain in detail with operation mode and its application. Draw the frame format of IPsec also. (5)

Q5 What is Wireless Sensor Networks? Explain various types of attacks on WSN. (5)

Q6 (a) Differentiate between Internal and external attack in MANET. (3)

(b) Differentiate between RREQ and Data Flooding attack in MANET. (2)

****