Registration No : □□□□□□□□□□

Total Number of Pages : 01 **B.Tech**

PCS7J001

7th Semester Regular / Back Examination 2019-20
CRYPTOGRAPHY & NETWORK SECURITY
BRANCH : CSE
Max Marks : 100
Time : 3 Hours
Q.CODE : HRB021

Answer Question No.1 (Part-1) which is compulsory, any eight from Part-II and any two from Part-III.

The figure s in the right hand margin indicate marks.

Part- I

Q1 **Only Short Answer Type Questions (Answer All-10)** **(2 x 10)**

a) What is known plain text attach? How it is different from chosen plain text attack.
b) Differentiate between confidentiality and integrity?
c) What is one-way trapdoor function? Give one example.
d) What are the symmetric and asymmetric encryptions?
e) What does you mean by Reply Attack?
f) Why network need security?
g) Explain cryptanalysis.
h) What is a threat? List some examples.
i) Mention services provided by PGP.
j) State the definition of intrusion detection.

Part- II

Q2 **Only Focused-Short Answer Type Questions- (Answer Any Eight out of Twelve)** **(6 x 8)**

a) Describe ceaser cipher and monoaphabetic cipher suitable examples.
b) Explain Fermat and Eluer’s Theorem.
c) Perform decryption and encryption using RSA algorithm with p = 3, q = 11, e = 7 and N=5.
d) Briefly explain Deffie Hellman key exchange with an example.
e) What is IDS? Explain the profile based IDS?
f) Explain about SSL Handshake protocol.
g) Explain the Chinese remainder theorem with an example.
h) Define virus. Explain in detail.
i) Define intrusion detection and the different types of detection mechanisms, in detail.
j) How Hash function algorithm is designed? Explain their features and properties.
k) Explain secure electronic transaction.
l) Write Short notes on S/MIME.

Part-III

Only Long Answer Type Questions (Answer Any Two out of Four)

Q3 Explain simplified DES with example. **(16)**

Q4 Describe MD5 algorithm in detail. Compare its performance with SHA-1. **(16)**

Q5 Explain the technical details of firewall and describe any three types of firewall with neat diagram. **(16)**

Q6 Explain the architecture of IP Security. **(16)**