Registration No : □□□□□□□□□□

Total Number of Pages : 01

B.Tech.
PCS7G002

7th Semester Regular Examination 2018-19
CRYPTOGRAPHY AND NETWORK SECURITY
BRANCH : CSE
Time : 3 Hours
Max Marks : 100
Q.CODE : E441

Answer Question No.1 (Part-1) which is compulsory, any EIGHT from Part-II and any TWO from Part-III.
The figures in the right hand margin indicate marks.

Part- I

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

a) Give the types of attack?
b) State Fermat's theorem.
c) What are the properties of hashing functions?
d) Distinguish between message integrity and message authentication.
e) How is the security of a MAC function expressed?
f) Write a simple authentication dialogue used in Kerberos.
g) Define Diffusion and Confusion.
h) What do you mean by shared secret key?
i) Write about the application of DES in CBC mode.
j) What is meant by intrusion detection?

Part- II

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

a) Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain.
b) What is Buffer Overflow? What are the tasks in exploiting the overflowable Buffer?
c) Given p = 19, q = 23, and e = 3 Use RSA algorithm to find n, φ(n) and d.
d) What are discrete logarithms? Explain how are they used in Public Key Cryptography?
e) Give the structure of HMAC. Explain the applications of HMAC.
f) List the evaluation criteria defined by NIST for AES.
g) List out the participants of SET system, and explain in detail.
h) Discuss the different methods involved in authentication of the source.
i) Name some viruses & explain it.
j) Explain the types of Host based intrusion detection. List any two IDS software available.
k) Write brief note on Web Security.
l) Describe about SSL/TLS Protocol.

Part-III

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

Q3 Explain in details about Triple DES and RC4. **(16)**

Q4 Explain in details about Diffie-Hellman Key Exchange. **(16)**

Q5 Illustrate about the SHA-1 algorithm in details. Compare its performance with MD5 and RIPEMD-160 and discuss its advantages. **(16)**

Q6 Explain the technical details of firewall and describe any three types of firewall with neat diagram.how they prevent intrusions. **(16)**