Registration No :

Total Number of Pages : 01

B.Tech
PCS7G002

7th Semester Regular / Back Examination 2019-20
CRYPTOGRAPHY & NETWORK SECURITY
BRANCH : CSE
Max Marks : 100
Time : 3 Hours
Q.CODE : HRB346
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 **Only Short Answer Type Questions (Answer All-10)** **(2 x 10)**
a) Distinguish between cryptography and Steganography.
b) Define integrity in Security.
c) What is transposition cipher and how it is different from the substitution cipher?
d) What is the key size of affine cipher in Z_{26}?
e) Find the value of $\Phi(81)$ using Euler's Phi-function.
f) Mentioned the differences between symmetric and asymmetric-key cryptosystems.
g) Compare conventional signature and a digital signature.
h) What is message digest and why it is used?
i) What do you mean by a cryptographic hash function?
j) What is a worm and what are its effects?

Part- II

Q2 **Only Focused-Short Answer Type Questions- (Answer Any Eight out of Twelve)** **(6 x 8)**
a) What is additive cipher and what is possible key size? Encrypt "CRYPTOGRAPHY" with Key=7.
b) Find the GCD of (25, 60) using the Euclidean algorithm.
c) Write both versions of Fermat's little theorem? Calculate 3^{12} mod 11.
d) Write the Chinese remainder theorem with all steps.
e) Explain improved Fiestal cipher with diagram.
f) Write the encryption, decryption, and key generation of Elgamal cryptosystem.
g) Explain MIME in E-mail security.
h) List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512.
i) What is man in the middle attack? Write Diffie-Hellman key exchange algorithm.
j) Explain all steps of the Vigenere cipher by taking a suitable example.
k) Explain briefly about PKI using proper diagram.
l) What is a digital signature? Why it is used?

Part-III

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

Q3 What do you mean by Hill cipher? Explain the Hill cipher using suitable example. **(16)**

Q4 Explain simplified DES with all its components. **(16)**

Q5 What is a firewall and what are its types? Explain the design techniques. **(16)**

Q6 What is MAC and how it is different from MDC? Explain about SHA-512. **(16)**