

BACHELOR OF TECHNOLOGY (C.B.C.S.) (2014 COURSE)
B.Tech.Sem - VIII IT :SUMMER- 2022
SUBJECT : NETWORK SECURITY & CRYPTOGRAPHY

Day : Wednesday
Date : 22-06-2022

S-13442-2022

Time : 02:30 PM-05:30 PM
Max. Marks : 60

N.B.:

- 1) All questions are **COMPULSORY**.
 - 2) Figures to the right indicate **FULL** marks.
 - 3) Draw neat labeled diagrams **WHEREVER** necessary.
 - 4) Assume suitable data if necessary.
-

Q.1 Discuss the Classical cryptosystem and its types. **(10)**

OR

Q.1 State and prove Euclids algorithm with suitable example. **(10)**

Q.2 Explain the OSI security architecture along with services available. **(10)**

OR

Q.2 Illustrate various Transposition techniques in detail. **(10)**

Q.3 Briefly explain s design principles of Block cipher. Discuss in detail Block cipher modes of operation. **(10)**

OR

Q.3 Elaborate Public key cryptosystems with an example. **(10)**

Q.4 How Hash function algorithm is designed? Explain its features and properties. **(10)**

OR

Q.4 List the properties of Digital signature and explain Digital Signature process and its standards. **(10)**

Q.5 Why E-commerce transaction need security? Which tasks are performed by payment gateway in E-commerce transactions? Explain the SET (Secure Electronic Transaction) protocol. **(10)**

OR

Q.5 Describe the various types of Intrusion Detection System (IDS). What are the Active and Passive IDS? **(10)**

Q.6 Draw the block diagram for structure of PGP message generation, and write about the usage of session keys, public and private keys in PGP. **(10)**

OR

Q.6 What is need of SSL? List the functions of different protocols of SSL. Explain the handshake protocol in detail. **(10)**

* * * *