B. Tech. Sem - VIII (Inf. Tech.) (2014 COURSE) (CBCS) :
SUMMER - 2019
SUBJECT: 3) ELECTIVE – III NETWORK SECURITY & CRYPTOGRAPHY

Day: Saturday
Date: 01/06/2019

Time: 02.30 PM TO 05.30 PM
Max Marks. : 60

S-2019-2914

N.B.:

1) All questions are **COMPULSORY**.
2) Figures to the right indicate **FULL** marks.
3) Assume suitable data, if necessary.
4) Use of non programmable calculator is **ALLOWED**.
5) Draw neat and labeled diagrams **WHEREVER** necessary.

Q.1 Summarize need of network security. Discuss the relation between security mechanisms and attacks in detail. **(10)**

OR

Q.1 Write about Fermat and Euler's theorem in detail. **(10)**

Q.2 Describe the CNSS security Model, with its three dimensions. **(10)**

OR

Q.2 With suitable examples, distinguish between transposition cipher system and substitution cipher system. **(10)**

Q.3 Draw the structure of AES. Explain how Encryption and decryption is done in AES. **(10)**

OR

Q.3 Discuss the RSA algorithm in detail, with its computational aspects and security. **(10)**

Q.4 Briefly explain the different message authentication functions with neat diagram. **(10)**

OR

Q.4 Explain Digital signature with ElGamal public key cryptosystem with example. **(10)**

Q.5 Write in detail about definition, characteristics, types and limitations of Firewall. **(10)**

OR

Q.5 How will you enhance the ability of a system to defend against intruders and malicious program? **(10)**

Q.6 Illustrate the confidentiality and authentication service provided by PGP. **(10)**

OR

Q.6 Elaborate the architecture of IP Security with neat diagrams. **(10)**

* * * * * *