EX/IT/T/322/2018

BE IT 3rd Year 2nd Semester Examination, 2018

CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 Hours

FULL MARKS: 100

Answer Any **FIVE** Questions

1.a) With regard to the X.800 standard, explain what are those security mechanism required to provide the "Traffic Flow Confidentiality" service to the user.

b) With proper example, explain the principles of "Unforgettable Substitution Cipher".

c) Using proper diagram, explain how round keys are generated in DES.

d) With proper diagram, explain how SHA-512 Hash algorithm works.

(4+4+4+8)

2.a) Using proper examples, explain the principles of Stream Cipher.

b) Using proper numerical examples, explain Lagrange's Theorem.

c) Using proper numerical examples, explain how Man-in-the-Middle attack occurs for Diffie-Hellman Key Exchange algorithm.

d) Explain how Decryption works for the Rabin Cryptosystem.

(4+4+5+7)

3.a) Explain briefly the attacks on RSA.

b) Using proper illustration, explain the geometric approach of adding two points on an elliptic curve.

c) Using proper example, explain "Elliptic Curve Discrete Logarithm Problem".

d) With proper illustration, explain the concept of Direct Digital Signature.

(4+6+5+5)

4.a) List down the parameters which constitute the Connection State in SSL.

b) Explain the parameters which get exchanged during the Handshake Protocol in SSL.

c) Explain the concepts and advantages of Tunnel Mode in IPSec.

d) With proper diagram, explain how Outbound Packet Processing is done in IPSec. (5+5+(3+2)+5)

5.a) Explain different types of Firewall.

b) With proper diagram, explain how Confidentiality & Authentication operation takes place in PGP.

c) With proper diagram, explain the message format in PGP

d) In PGP, explain how Trust Model works. (6+6+4+4)

6.a) List down 6 different Intrusion Technique.

b) Discuss how Intrusion can take place using Password.

c) Explain the following terminologies related to Malicious Program:-
Virus, Worm, Logic Bomb, Trojan Horse.

d) Discuss the evolution of Anti-Virus Solution.

(4+4+6+6)