BE IT 3rd Year 2nd Semester Examination, 2019

CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 Hours FULL MARKS: 100

Answer Any **FIVE** Questions

1.a) What is Denial of Service Attack? Explain how this can be prevented.

b) How 'Key Space' is different in Caesar Cipher, Shift Cipher and Substitution Cipher? Explain with example?

c) Using proper diagram, explain how Key Streams are generated in RC4?

d) With proper diagram, explain how S-box works in DES.

((2+3)+(3+2)+5+5)

2.a) Using proper examples, explain the problem of 'Birthday Attack'.

b) Comet 2P/Encke, 4P/Faye and 8P/Tuttle have orbital period of 3 years, 8 years and 13 years respectively. The last perihelions of each of these comets were in 2017, 2014 and 2008 respectively. What is the next year in which all three of these comets will achieve perihelion in the same year?

For this problem, assume that time is measured in whole numbers of years and that each orbital period is constant.

c) With respect to Diffie-Hellman Key Exchange algorithm, a malicious user can make the server quite busy by continuously sending half-key; thus making the server continuously computing the full-key and send it back to user. What is the name of this attack? How this kind of attacks can be prevented?

d) What is that mathematical concept, based upon which the ElGamal Cryptosystem works? Explain this concept with example.

(5+5+(1+4)+(1+4))

3.a) Using proper numerical example, explain RSA.

b) Using proper illustration, explain the geometric approach of doubling a point on an elliptic curve.

c) Using proper illustration, explain how MAC can be used for Authentication.

d) With proper illustration, explain the concept of Arbitrated Digital Signature. (5+5+5+5)

4.a) Using proper diagram, explain the architecture of SSL protocol stack.

b) Explain the creation of Master Secret with respect to SSL.

c) List down the Services offered by IPSec.

d) List down the Encryption Algorithm used in IPSec. (5+5+5+5)

5.a) Explain what a Firewall does.

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

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

d) With proper illustration, explain PGP Key Rings. (4+6+4+6)

6.a) Explain 3 types of Intruder Behavior Patterns.

b) List down 8 'Measures' that may be used for Intrusion Detection.

c) Explain the following terminologies related to Malicious Program:-
Backdoor or Trapdoor, Keyloggers, Rootkit, Exploits

d) With proper illustrations, explain Digital Immune System. (6+4+4+6)