

B. E. Computer Science & Engineering**FOURTH YEAR, FIRST SEMESTER EXAMINATION 2019****COMPUTER AND NETWORK SECURITY**

Time: 3 hours

Full Marks: 100

Group A (Total Marks: 25) [CO1]Answer Question No. 1 OR Question no. 2.

1. a) What are the aspects of security? Briefly explain.
 b) What are meant by *masquerading*, *snooping*? What threat categories do each of these belong to?
 c) What is hash function? What are the desirable properties of hash function?
 d) How does Symmetric Key Cryptosystem work?
 e) What is *Attribute based access control*? 6+6+6+4+3=25

2. a) What is security?
 b) What is *threat*? What are the different broad categories of threat? Explain briefly any two of them with suitable examples.
 c) How is the (*public*, *private*) key pair generated using RSA algorithm?
 d) What is MAC used for? How does it work?
 e) What is *Role based access control*? 3+8+5+6+3=25

Group B (Total Marks: 35) [CO2]Answer Question No. 3 OR Question no. 4.

3. a) Explain in details the working of *Kerberos*.
 b) What is *security association* in IPsec? How is it handled?
 c) What are the modes of operation of IPsec?
 d) Mention any three algorithms that IPsec uses and their respective usages.
 e) What *keys* are used in Pretty Good Privacy (PGP)? How does PGP compress files? When is the signature generated and messages encrypted?
 f) What does S/MIME provide? What are the different content types in S/MIME? 8+4+5+6+6+6=35

4. a) What is *Kerberos*? What are its drawbacks?
 b) What are the header fields in S/MIME? How can S/MIME be used for secrecy and authentication?
 c) How is confidentiality maintained in Pretty Good Privacy (PGP)?
 d) What does *Transport Layer Security* (TLS) provide? What are the different security measures provided by TLS? Explain the working of the TLS Record protocol. What is *cipher suite*? For what purposes are *public key* algorithms used in TLS? 5+8+5+(3+5+4+3+2)=35

[Turn over

Group C (Total Marks: 20) [CO3]

5. Answer ANY TWO questions: 2X10=20
- a) How does *virus* work? What is *firewall*? (6+4=10)
- b) What is *spyware*? What are its different types? Explain. (2+8=10)
- c) What is *intrusion detection system*? What are its goals? Explain the working of *Host intrusion detection system* (HIDS). (2+3+5=10)
- d) How is *Virtual private network* (VPN) created? What is the function of *Network intrusion detection system* (NIDS)? (4+6=10)

Group D (Total Marks: 20) [CO4]

6. Answer ANY TWO questions: 2X10=20
- a) How is Win XP user authentication performed? What is not supported by the file system of Win CE? (5+5=10)
- b) What are the keystroke dynamics? Why are these considered to be unique? What is *Pass algorithm*? (4+3+3=10)
- c) How does *challenge response* mechanism work? Briefly explain the *hardware supported challenge response* procedures. (5+5)=10
- d) What security features are expected of an operating system? What is *Protection key mechanism*? (6+4=10)
- e) What are the objectives of the IT Act 2008? Why are state governments given the power to make rules? (7+3=10)
- f) Mention any two offences and the corresponding punishments as mentioned in Section 66. (2X5=10)
-