CSE 413 (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

IV/IV B.Tech. DEGREE EXAMINATIONS, NOVEMBER- 2019

First Semester

COMPUTER SCIENCE ENGINEERING

CYBER SECURITY

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory **6X2=12 M**

Answer ONE Question from each Unit **4X12=48 M**

1. a) Differentiate threat and attack

   b) State Euler’s theorem

   c) What is message authentication?

   d) State the difference between conventional encryption and public-key encryption.

   e) Concept of Mobile hacking

   f) Name any two security standards

UNIT-I

2. a) Explain the characteristics of block and stream ciphers.

   b) Explain the concept of Stegnography and give its applications and limitations

(OR)

3. Give the overall structure of the AES encryption process. Describe the sequence of transformations in each round and showing the corresponding decryption function.

UNIT-II

4. a) What is Public Key certificate? Explain its usage with X.509 certificates.

   b) Explain in detail Digital Signature Standard approach and its algorithm.

(OR)

5. a) In what way Diffie Hellman key exchange algorithm prone to man in the middle attack? Explain.

P.T.O

b) With a neat sketch explain overview of Message Exchanges in Kerberos version 5.

UNIT-III

6. a) Describe about SSL secure communication and SSL authentication.

   b) Describe the various modes of arbitrated digital signatures.

(OR)

7. a) What services are provided by IPSec? Explain.

   b) Write the general format of PGP Message. Explain the PGP message generation from User A to User B with no compression.

UNIT-IV

8. a) What is intruder? Explain the Intrusion detection System in detail. Elaborate on types of intruders.

   b) Give a brief on Malicious Software types.

(OR)

9. a) Give a brief on Firewall, its characteristics and elaborate on its types.

   b) Explain about UNIX Password Management.

CSE 413 (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

IV/IV B.Tech. (Supple) DEGREE EXAMINATIONS, JUNE- 2019

First Semester

COMPUTER SCIENCE ENGINEERING

CYBER SECURITY

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory **6X2=12 M**

Answer ONE Question from each Unit **4X12=48 M**

1. a) What is a security attack?

   b) What is meant by Denial of Service (DOS)

   c) List out the problems of one time pad?

   d) What is Public Key certificate?

   e) What is a worm?

   f) What is meant by stateful packet inspection?

UNIT-I

2. a) Determine the security mechanisms required to provide various types of security services.

   b) Explain symmetric cipher model with neat block diagram.

(OR)

3. a) Explain in detail the sub key generation and round function of DES algorithm in detail.

   b) What is session hijacking? Explain about TCP/IP session hijacking in d etail.

UNIT-II

4. Discuss the following related to Elliptic Curve Cryptography (ECC)

   a) ECC Encryption/Decryption and Security of ECC

   b) ECC Diffie Hellman Key Exchange.

P.T.O

(OR)

5. a) Perform encryption and decryption using the RSA algorithm P=3, q=11, e=7, M=5.

   b) Explain Digital Signature Scheme (DSS) and Digital Signature Algorithm (DSA) in detail.

UNIT-III

6. a) Write note on PGP session keys, public/private key rings and passphrase keys.

   b) Describe the SSL Architecture in detail.

(OR)

7. a) Expalin ISAKMP protocol.

   b) Give a brief on Web Security and explain Alert and Handshake protocols.

UNIT-IV

8. a) Explain different types of IDS

   b) Give a brief on VoIP and Wireless hacking.

(OR)

9. a) Give a brief on firewell, its benefits and limitations. Explain the firewall architecture.

   b) Explain the need for trusted systems.