PVP 19

Code: 19CS4601B

III B.Tech - II Semester – Regular Examinations – JUNE 2022

CRYPTOGRAPHY AND INFORMATION SECURITY
(COMPUTER SCIENCE & ENGINEERING)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 5 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each question carries 12 marks.
4. All parts of Question paper must be answered in one place.

PART – A

1. a) Define Data Confidentiality.

b) Write about message digest.

c) Compare session key and a master key.

d) Describe about Handshake protocol.

e) Explain IP Hijacking.

PART – B
UNIT – I

2. a) With the help of neat diagrams explain about symmetric key ciphers in detail. 6 M

b) Illustrate IDEA algorithm in detail. 6 M

OR

3. a) Write a note on different types of security services and attacks in detail. 6 M

b) Explain about OSI Security architecture model with neat diagram. 6 M

UNIT – II

4. a) Illustrate SHA-512 algorithm in detail. 6 M

b) Discuss digital signature standard with necessary diagrams in detail. 6 M

OR

5. a) Assume in an authentication scheme, the hash function used is H and encryption/decryption function is E/D. Show how the function will be used to provide authentication as well as confidentiality. 6 M

b) List and explain what characteristics are needed in a secure hash function. 6 M

UNIT-III

6. a) What are the core components of a PKI? Briefly describe each component. 6 M

b) Explain the problems with key management and how it affects symmetric cryptography. 6 M

OR

7.	a)	Discuss in detail about Symmetric Key Distribution Using Symmetric Encryption with an example.	6 M
	b)	Explain briefly about the architecture and certification mechanism in X.509 in detail.	6 M

UNIT – IV

8.	a)	Describe in detail about SSL/TSL.	6 M
	b)	Briefly discuss about Web Security Threats.	6 M

OR

9.	a)	Write the steps involved in the simplified form of the SSL/TSL protocol.	6 M
	b)	Write the methodology involved in computing the keys in SSL/TSL protocol.	6 M

UNIT – V

10.	a)	Explain PGP cryptographic functions in detail with suitable block diagrams.	6 M
	b)	List the major security services provided by AH (Authentication Header) and ESP (Encapsulating Security Payload), respectively.	6 M

OR

11. a) Discuss in detail about Internet Key Exchange- Key Determination Protocol. 6 M

b) The IPsec architecture document states that when two transport mode SAs are bundled to allow both AH (Authentication Header) and ESP (Encapsulating Security Payload) protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption? 6 M