ST.ANNE'S

COLLEGE OF ENGINEERING AND TECHNOLOGY

ANGUCHETTYPALAYAM, PANRUTI – 607106.

QUESTION BANK

JULY 2018 - NOV 2018 / ODD SEMESTER

BRANCH: CSE **YR/SEM:** IV/VII **BATCH**: 2015 - 2019

SUB CODE/NAME: CS6004 - CYBER FORENSICS

UNIT I - NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

1. Define IPsec Protocol.
2. Write the basic components of IPsec architecture Protocol.
3. Define IPsec Protocol Documents
4. Define Security Associations (SAs)
5. Define Hashed Message Authentication Code (HMAC)
6. Define IP Authentication Header.
7. Draw AH Format.
8. Define IP ESP.
9. Define Packet Format
10. Define Key Management Protocol for IPSec.
11. List out the different types of Payload Types for ISAKMP.
12. Define SSL Protocol.
13. Draw the SSL Protocol Overview stack.
14. Difference between SSL Session and SSL Connection.
15. List out the SSL session elements.
16. List out the SSL Connection elements.
17. Define SSL Record Protocol format.
18. List out the phases of SSL Handshake Protocol.
19. List out the ISAKMP Payload Processing.
20. Define Cryptographic Computations.

PART B

1. Explain in detail about the IPsec Protocol.
2. Explain in detail about the IP Authentication Header.
3. Explain in detail about the IP ESP.
4. Explain in detail about the Key Management Protocol for IPSec.
5. Explain in detail about the SSL protocol.
6. Explain in detail about the Cryptographic Computations
7. Explain in detail about the TLS Protocol.

UNIT II - E-MAIL SECURITY & FIREWALLS

Part-A

1.What is application level gateway?

2. List the design goals of firewalls?

3.What is mean by SET? What are the features of SET?

4. What are the steps involved in SET Transaction?

5.Define S/MIME?

6. What are the headers fields define in MIME?

7. What is MIME content type and explain?

8. What are the key algorithms used in S/MIME?

9. Give the steps for preparing envelope data MIME?

10.What are the services provided by PGP services

11. Explain the reasons for using PGP?

12. Why E-mail compatibility function in PGP needed?

13. Name any cryptographic keys used in PGP?

14.What is meant by S/MIME? (A/M-12)

15.List out the types of firewalls.

Part-B

1.Explain in detail about the PGP.

2.Explain in detail about the S/MIME.

3.Explain in detail about the Types of Firewalls in Internet Firewalls for Trusted System.

4. Explain in detail about the Firewall related terminology in Internet Firewalls for Trusted System.

5.Explain in detail about the SET for E-Commerce Transactions.

UNIT III - INTRODUCTION TO COMPUTER FORENSICS

Part-A

1.Define computer crime.

2. Define computer forensics.

3.List out the Traditional problems associated with Computer Crime.

4.Define identify theft.

5. Define Identity fraud.

6.List out the Typologies of Identity Theft/Fraud

7.List out the Physical Methods of Identity Theft

8.How to prepare a computer investigation.

9.What are the Steps for problem solving

10.Write the steps for Planning Your Investigation

11.List out the forensics technology.

12.List out the forensics system.

13.Draw the internet security hierarchy.

14.Define Intrusion Detection.

15.write the benefits of firewalls.

Part-B

1. Explain in detail about the Traditional problems associated with Computer Crime.

2. Explain in detail about the Introduction to Identity Theft & Identity Fraud.

3. Explain in detail about the Incident and incident response methodology.

4. Explain in detail about the Forensics Technology and Systems.

5. Discuss about the Understanding Computer Investigation.

6. Discuss about the Data Acquisition.

UNIT IV - EVIDENCE COLLECTION AND FORENSICS TOOLS

Part-A

1.Write the rule for the rules for controlling digital evidence.
2.Define Best evidence rule states:
3. Define Federal Rules of Evidence
4. How to collect evidence at private-sector incident scenes.
5. Define Processing Law Enforcement Crime Scenes
6.How to prepare for a search in criminal case.
7. Determining Whether You Can Seize Computers and Digital Devices in processing crime.
8.How are the tools are used in processing crime and incident scene.
9.How to prepare for a Preparing the Investigation Team
10.List out the Storing Digital Evidence.
11.How to Reviewing a Case.
12.Define file system.
13.List out the disk drive components.
14.Define Solid-State Storage Devices.
15.Define NTFS Encrypting File System (EFS)
16. Define NTFS Disks
17.Define Deleting NTFS Files
18.List out the Third-Party Disk Encryption Tools.
19. Explain how the Windows Registry works
20.List out the registry terminology.

Part-B

1. Explain the rules for controlling digital evidence
2. Describe how to collect evidence at private-sector incident scenes
3. Explain guidelines for processing law enforcement crime scenes
4. List the steps in preparing for an evidence search
5. Describe how to secure a computer incident or crime scene
6. Describe Microsoft file structures
7. Explain the structure of New Technology File System (NTFS) disks
8. List some options for decrypting drives encrypted with whole disk encryption
9. Explain how the Windows Registry works
10. Describe Microsoft startup tasks
11. Describe MS-DOS startup tasks
12. Describe available computer forensics software tools
13. List some considerations for computer forensics hardware tools
14. Describe methods for validating and testing computer forensics tools

UNIT V- ANALYSIS AND VALIDATION

Part-A

1. Define bit-shifting
2. Define Known File Filter (KFF).
3. Define steganography.
4. Define network forensics.
5. Define client/server architecture.
6. Define Enhanced Simple Mail Transfer Protocol (ESMTP).
7. Define Multipurpose Internet Mail Extensions (MIME)
8. Define spoofing
9. How to Validating with Computer Forensics Programs
10. List out the Addressing Data-hiding Techniques
11. Define Code Division Multiple Access (CDMA)
12. Define Electronically erasable programmable read-only memory (EEPROM)
13. Define fourth-generation (4G).
14. Define Global System for Mobile Communications (GSM).
15. Define Orthogonal Frequency Division Multiplexing (OFDM).
16. How to Exploring the Role of E-mail in Investigations.
17. How to Exploring the Roles of the Client and Server in E-mail.
18. List out E-Mail Headers.
19. List out the E-mail Forensics Tools
20. Define SIM Card Readers

Part-B

1. Determine what data to analyze in a computer forensics investigation
2. Explain tools used to validate data
3. Explain common data-hiding techniques
4. Describe methods of performing a remote acquisition
5. Explain standard procedures for network forensics
6. Describe the use of network tools
7. Describe the importance of network forensics
8. Explain the basic concepts of mobile device forensics
9. Describe procedures for acquiring data from cell phones and mobile devices
10. Explain in detail about the E-Mail Investigations.