Purple = P1
Orange = P2
Green = P3
Blue = P4

C.S.S

MODULE-1

1. Encrypt " academic committee will meet today " using Playfair cipher with Keyword "ROYAL ENFIELD".
2. Enlist security goals. Discuss their significance.
3. What are traditional ciphers? Discuss any one substitution and transposition cipher with example. List their merits and demerits.
4. Discuss in detail block cipher modes of operation.
5. Summaries and find Plain text by decrypting ciphertext "XVWG" using Hill Cipher Substitution Technique.
6. Use Hill cipher to encrypt the text "short". The key to be used is "hill".
7. With the help of suitable examples compare and contrast monoalphabetic ciphers and polyalphabetic ciphers?
8. Use the Play fair cipher with the keyword:"MEDICINE" to encipher the message "The greatest wealth is health."

MODULE-2

1. Elaborate international Data encryption Algorithm(IDEA) and its key generation?
2. With reference to DES comment on the following i) Block size and key size ii) Need for expansion permutation iii) Avalanche and completeness effects iv) Weak keys and semi-weak key v) Role of S-box
3. Compare AES and DES. Which one is bit oriented? Which one is byte oriented?
4. Numerical on Diffie-Hellman key exchange technique.
5. Write a short note on 1) 3DES 2) Session Hijacking and Spoofing 3) Blowfish

6. Discuss CBC and OFB Block cipher Modes with examples.

7. Numerical on Convert given using S-DES Algorithm.

8. Explain the concept of Key management along with its Distribution System.

9. What is the purpose of S-boxes in DES? Explain the avalanche effect?

10. Encrypt the message "Cryptography is fun" with a multiplicative cipher with key- 15. Decrypt to get back original plaintext.

11. What are the different threats to emails? Give an algorithm to secure emails being sent from user A to user B.

12. Compare Block and stream ciphers

13. Compare Key generation in IDEA and Blowfish

14. Briefly define idea behind RSA and also explain. 1) What is the one way function in this system? 2) What is the trap door in this? 3) Give Public key and Private Key. 4) Describe security in this system.

15. Explain DES, detailing the Feistel structure and S-block Design.

16. Consider a Voter data management system in E-voting system with sensitive and non-sensitive attributes. 1) Show with sample queries how attacks are possible on such data sets (Direct, Interface) 2) Suggest 2 different ways to mitigate the problem.

17. Explain Diffie-Hellman Key exchange algorithm with suitable example. Also explain the problem of MIM attack in it.

18. What are the various ways in which public key distribution is implemented. Explain the working of public key certificates clearly detailing the role of certificate authority.

19. Timing and Storage Covert Channel

MODULE-3

1. What are the requirements of the cryptographic hash functions? Compare MD5 and SHA Hash functions. State real world applications of hash functions.

2. Write a short note on 1) X.509 2) SHA-1

3. Explain Hash Based Message Authentication Code.Give examples also.

4. List and explain various types of attacks on encrypted message.

5. What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block.

6. What are the properties of hash function? What is the role of hash function in security.

7. Compare MD-5 versus SHA

MODULE-4

1. What is a digital certificate? How does it help to validate the authenticity of a user? Explain the X.509 certificate format. OR Explain Digital Signature and Digital Certificate used for Authentication? OR Why are Digital Signatures & Digital certificates required? What is the significance of Dual Signature.

2. Kerberos OR Explain Kerberos protocol that supports authentication in distributed system.

3. Consider a scenario where an intruder wants to access some valuable information from an ongoing communications.What security service should be implemented in system and which mechanism can be used to achieve those security services.

4. Numerical on Calculate Cipher text using RSA Algorithm.

5. What is authentication header(AH)? How does it protect against replay attacks? OR What is the need for message authentication? List various techniques used for message authentication. Explain any one.

6. Why E-Commerce transactions need security? Which tasks are performed by payment gateway in E-commerce transaction? Explain the SET (Secure Electronic Transaction) protocol.

7. Numerical on Calculate their private keys.

8. Write a short note on S/MIME

MODULE-5

1. Explain the different types of Denial of Service attacks. OR What are Denial of Service attack ? Explain any three types of DOS attacks in detail.

2. What is the need of SSL? Explain all phases of SSL Handshake protocol in detail.

3. Differentiate between i) MD-5 and SHA ii) Firewall and IDS. OR What are the types of Firewalls? How are firewalls different from IDS.

4. What are the different protocols in SSL? How do the client and server establish an SSL connection.

5. Describe various types of Instruction Detection System(IDS).What are Active and Passive IDS?

6. Why is the segmentation and reassembly function in PGP (Pretty Good Privacy) needed?

7. How can we achieve web security? Explain with example.

8. Explain IPSec protocol in detail. Also write applications and advantages of IPSec.

9. What are the various ways and address protecting Operating System?

10. How is security achieved in the transport and tunnel modes of IPSec? What are security associations?

11. What are the different components of an Intrusion Detection System? Compare the working of signature based IDS with. anomaly based IDS.

12. Explain key rings in PGP.

13. IPSec offers security at n/w layer. What is the need of SSL?. Explain the services of SSL protocol?

MODULE-6

1. Explain briefly with examples, how the following attacks occur: i) Phishing attack ii) Denial of Service attack iii) SQL injection attack iv) Cross-site scripting attack v) Buffer Overflow

2. List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack.

3. Give examples of replay attacks. List three general approaches for dealing with replay attacks.

4. What are the different types of viruses and worms ? How do they propagate?