QUESTION BANK

MODULE 1

Chapter 1(Introduction)

1. Explain the motives of launching ***cyber attacks.***
2. Explain the ***types of attacks/common attacks launched /high profile attacks.***
3. Define ***vulnerability***. Explain the ***types of vulnerabilities*** in the domain of Security.
4. Briefly explain the ***defence strategies*** and techniques deployed to overcome network attacks.
5. Explain ***access control,authentication and authorization.***
6. Explain the ***guiding principles*** in security practice.

Chapter 2(Mathematical Background for cryptography)

7. Explain the ***properties ofmodulo arithmetic.***
8. Solve using ***euclids algorithm*** for gcd(161,112)
9. Explain the ***extended euclids algorithm*** pseudocode along with illustration of this example b=79 and c= 12

   Or

   Find the ***inverse of 12 modulo 79.***
10. Define group and explain the properties of group.
11. Define lagranges theorem,eulers, fermats little theorem.
12. Consider the group <Z 13,*13>, is it a cyclic group. check whether 2 is a generator of Z 13.
13. Explain Chinese remainder theorem.
14. Problem on Chinese remainder theorem

Chapter 3(Basics Of Cryptography)

15. Define **a)cryptography b) ciphertext c) encryption d)decryption e)kerchoffs principle.**
16. Bring out the difference between **secret key cryptography and public key cryptography.**
17. Explain ***known ciphertext attack*** with a pseudocode.
18. Explain the ***types of elementary substitution ciphers*** with example.
19. Explain ***monoalphabetic ciphers*** with example.
20. Explain ***all polyalphabetic ciphers*** methods with an example.
21. Explain ***hill cipher ,vigenere cipher and one time pad cipher methods*** with example.
22. What are ***transposition ciphers.*** explain the working of it with an example.
23. Differentiate between ***confusion and diffusion.***
24. Write a note on ***stream and block cipher.***

Chapter 4(Secret Key Cryptography)

25. Demonstrate the working of a **product cipher** with a neat figure.

    OR

    Explain **Three Round SPN Network /**
26. Explain **DES algorithm**(along with round function)./ orExplain **Fiestel cipher structure**.
27. Explain ***S- box implementation*** using table look up,(substitution in round function)

MODULE 2

Chapter 1(Public key cryptography)

1. Explain ***RSA operations/ RSA key generation/algorithm/RSA encryption and decryption.***
2. Perform encryption and decryption using RSA algorithms for prime numbers p=3,q=11,e=3,and message = 011101011.
3. Explain ***RSA applications and performance.***

Chapter 2(cryptographic hash)

4. Explain ***weak and strong collision attack.***
5. Define hashing.Illustrate the ***properties of cryptographic hash*** with a neat figure.
6. Explain ***attack complexity OR weak collision and strong collision resistance*** *with a* ***pseudocose/program***
7. Explain the computation of ***generic cryptographic hash*** with a neat figure.
8. Explain ***MAC / message authentication code***. // (refer notes :explain the introduction part of HMAC)
9. Explain ***HMAC OR (Hash Based Message Authentication Code).***
10. Explain ***the computation of hash using SHA-1 OR SECURE HASH ALGORITHM -1.***
    OR
    Explain **Array Initialization And Hash Computation In Sha-1.**
11. Explain ***Digital signature*** .
12. Explain birthday analogy and attack.

Chapter 3(discrete logarithm and its applications)

13. Explain ***elgamal signature algorithm*** .
14. Explain ELgamal encryption
15. Perform encryption and decryption using El Gamal algorithm for a plaintext message 3 and assume p=11,g=2,receipeints private key a=5,and random number chosen by sender is 7 .
16. Explain **Diffie hellman key exchange algorithm / key exchange**
17. Explain man in the middle attack on **Diffie hellman key exchange algorithm.**
18. Compute the partial keys and shared secret keys using diffiehellman algorithms for the values g= and p= , random values a= , b =

MODULE 3

Chapter 1(Key management)

1. Explain digital certificates
2. Explain the format of X.509 certificate with a neat figure.
3. Explain public key infrastructure or functions of PKI
4. Explain the types of PKI Architecture.
5. Explain certificate revocation
6. Explain the identity-based encryption.

Chapter 2 (Authentication I)

7. Explain ***one-way authentication method*** **OR** **password-based authentication** technique.
8. Explain ***certificate-based authentication technique***.
9. **Explain shared secret-based authentication**
10. **Explain asymmetric key based authentication.**
11. **Explain authentication and key agreement using session key.**

    (OR) explain *mutual authentication* methods(all the above three, figure are must for each of these).

12. What are ***dictionary attacks*** and how an attacker would implement this attack.
13. How to defeat dictionary attack using ***EKE protocol.***

Chapter 3 (Authentication II)

14. Write a note on ***centralized authentication /message confidentiality using KDC.***
15. Explain **Needham Schroeder protocol version 1 and 2** along with the attacks launched on these versions.
16. Explain **Needham Schroeder protocol version 3** along with the attacks launched on this versions and final version.
17. Explain Needham Schroeder protocol Network Security & Cryptography Module 1 Prof.
18. Demonstrate the working of a **Kerberos protocol with a neat figure.**
19. Write a note on characteristics of biometrics and features of **fingerprints ,irisscan.**

Chapter 4 (IP security)

20. Explain IPSec protocols in **transport mode** with a neat diagram.
21. Explain IPSec protocols in **tunnel mode** with a neat diagram.
22. Explain **IKE phase 1 main mode**protocol with description of messages exchanged between the entities.
23. Explain **IKE phase 1Aggressive mode** protocol with description of messages exchanged between the entities.
24. Explain **IKE phase 2 protocol.**

Chapter 5(security at transport layer)

25. Explain **SSL handshake protocol**. /how a client and a server communicate using SSL handshake protocol
26. Explain the **key design ideas.**
27. Explain **SSL record layer protocol** with a neat figure.

MODULE 4

Chapter 1(IEEE 802.11 Wireless LAN security)

1. Explain the ***infrastructure of WLAN/wireless LAN*** .
2. Explain ***authentication in WEP and 802.11i.***
3. Explain ***key hierarchy*** and ***four way handshake protocol in 802.11i***
4. Explain ***TKIP*** with figure

5. Explain ***MAC generation and encryption in CCMP protocol*** with a neat schematic diagram.

Chapter 2(virus worms and other malware)

6. Explain the characteristics /features of virus and worms.
7. Explain internet scanning worms.
8. Explain ***Email And P2p Worms or explain topological worms.***
9. Write a note on ***web worms.***
10. Explain ***mobile malwares***.
11. Explain ***botnets with a neat figure***

Chapter 3(firewalls)

12. Explain the ***classification /types of firewalls*** based on the processing modes.
13. Explain functionalities , policies and access control lists.
14. Explain ***firewall ruleset./configuration***
15. Explain the significance of DMZ in placement of firewall with a neat diagram. (6M)

Chapter 4(Intrusion Prevention and Detection)

16. Explain the ***types of Intrusion detection system .***
17. Explain **IP traceback using Probablistic Packet marking and packet logging** with an example.
18. Explain DDos attack detection and prevention methods.

Chapter 5(Web Services Security)

19. Explain **entities involved in web services**
20. Write a note on XML with an example.
21. Explain ***SOAP framework***
22. Explain ***SAML and assertion types.***
23. Explain ***XML signature elements*** and sub elements with an example code

MODULE 5

1. Explain any four important provisions of IT act 2000
2. Describe the role of certifying authority with regard to issuing digital certificate and Representation upon issuance,suspension .
3. Who is a controller? Outline his functions as a controller.
4. Discuss the penalties and adjudication under section 43 IT act 2000 for

    a) Damage to computer, computer system
    b) Failure to protect data.
    c) Failure to furnish information return
5. Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000
6. Define the following terms:
    1. Certifying Authority b)Addressee c) Digital signature d)Public key
7. Explain offense ,punsishments ,penalties under IT act 2000.
8. Explain aim and objectives of IT act 2000.