**ORAL QUESTIONS ON ASSIGNMENT -1**

|  |  |
| --- | --- |
| **1.** | Explain RSA algorithm |
| **2.** | Explain security of RSA algorithm |
| **3.** | How do you generate key pair using RSA |
| **4.** | Why prime number used in RSA |
| **5.** | Explain Eular’s Totions function |
| **6.** | What is relatively prime number |
| **7.** | Explain difference between public key cryptography and symmetric cryptography |
| **8.** | Can RSA solve key distribution problem |

**ORAL QUESTIONS ON ASSIGNMENT-2**

|  |  |
| --- | --- |
| **1.** | Explain Extended Euclidean algorithm |
| **2.** | What is Chinese remainder therom |
| **3.** | Explain difference between Euclidean algorithm and Extended Euclidean algorithm |
| **5.** | What is the use of Extended Euclidean in RSA |
| **6.** | Explain Modulo arithmetic |

**ORAL QUESTIONS ON ASSIGNMENT-3**

|  |  |
| --- | --- |
| **1.** | What is password based authentication |
| **2.** | What is one way authentication |
| **3.** | What is mutual authentication |
| **4.** | What is socket |
| **5.** | How do we perform authentication using socket |
| **6.** | Explain challenge response protocol |
| **7.** | What is certificate based authentication |
| **8.** | What is shared secrete based authentication |
| **9.** | Explain dictionary attack |
| **10.** | What is asymmetric key based athentication |

**ORAL QUESTIONS ON ASSIGNMENT-4**

|  |  |
| --- | --- |
| **1.** | Explain MD5 algorithm |
| **2.** | Explain SHA1 algorithm |
| **3.** | What is disadvantages of MD5 |
| **4.** | Why sha1 is stronger that md5 |
| **5.** | What is message digest |
| **6.** | What is hash function explain its properties |
| **7.** | What is birthday attack |
| **8.** | What is initialization variable |
| **9.** | How much digest size of md5 |
| **10.** | How do we achieve data integrity using md5 or sha1 |

**ORAL QUESTIONS ON ASSIGNMENT-5**

|  |  |
| --- | --- |
| **1.** | What is AES? |
| **2.** | How much size of plaintext in AES |
| **3.** | Explain construction of AES |
| **4.** | How do we perform column mixing in AES |
| **5.** | Explain round key addition |
| **6.** | When do we perform byte substitution |

**ORAL QUESTIONS ON ASSIGNMENT-6**

|  |  |
| --- | --- |
| **1.** | What is engine class? |
| **2.** | Explain java cryptography architecture |
| **3.** | Explain cipher and key pair class. |
| **4.** | What is Algorithm Specific Interface |
| **5.** | Which class required for generation of Key pair for RSA |

**ORAL QUESTIONS ON ASSIGNMENT-7**

|  |  |
| --- | --- |
| **1.** | What is the use of wireshark? |
| **2.** | How do we monitor network using wireshark |
| **3.** | What is hex dump |
| **4.** | Is wireshark act as IDS tool |
| **5.** | What are filtering method of Wireshark |
| **6.** | Why do we capture packet in wireshark |
| **7.** | Is wireshark hacking tool |

**ORAL QUESTIONS ON ASSIGNMENT-8**

|  |  |
| --- | --- |
| **1.** | What is open port? |
| **2.** | What do you mean vulnerability of any system |
| **3.** | Describe Nessus security tool |
| **4.** | Explain the security hole |
| **5.** | Describe detail procedure of port scanning |
| **6.** | What are the nessus report specifies |

**ORAL QUESTIONS ON ASSIGNMENT-9**

|  |  |
| --- | --- |
| **1.** | What is snort? |
| **2.** | Explain how to configure snort on windows |
| **3.** | What is Rule based IDS and network based IDS |
| **4.** | Explain sniffer mode of snort |
| **5.** | What is packet logger mode |
| **6.** | What is TCP dump |
| **7.** | Is snort useful for forensic analysis tool |
| **8.** | What is the use of alert file |
| **9.** | What is the role of dymanic engine and preprocessor in snort |

**ORAL QUESTIONS ON ASSIGNMENT-10**

|  |  |
| --- | --- |
| **1.** | Explain SSL protocol |
| **2.** | What is PGP Tool |
| **3.** | What are different services provided by PGP |
| **4.** | What is the use of digital certificate |
| **5.** | Explain x.509 protocol |

General Questions

1. What are the essential ingredients of a symmetric cipher?
2. What are the two basic functions used in encryption algorithms?
3. How many keys are required for two people to communicate via a   
   cipher?
4. What is the difference between a block cipher and a stream cipher?
5. What are the two approaches to attacking a cipher?
6. What is the difference between an unconditionally secure cipher and   
   a computationally secure cipher?
7. Briefly define the Caesar cipher.
8. Briefly define the monoalphabetic cipher?
9. Briefly define the playfair cipher.
10. What are the two problems with one-time pad?
11. What is a transposition cipher?
12. What is Steganography?
13. What is the difference between diffusion and confusion?
14. What is the purpose of the S-boxes in DES?
15. Explain the avalanche effect.
16. What is the difference between a mono alphabetic cipher and a poly   
    alphabetic cipher?
17. List the types of cryptanalytic attacks.
18. What is the difference between differential and linear   
    cryptanalysis?
19. How is the S-box constructed?
20. Briefly describe Mix Columns.
21. Briefly describe Add Round Key.
22. Briefly describe the Key Expansion Algorithm.
23. What is the difference between Sub Bytes and Sub Word?
24. What is triple encryption?
25. What is a meet-in-the-middle attack?
26. How many keys are used in triple encryption?
27. What is the key size for Blowfish?
28. What types of information might be derived from a traffic analysis   
    attack?
29. What is traffic padding and what is its purpose?
30. List ways in which secret keys can be distributed to two   
    communicating parties.
31. What is the difference between a session key and a master key?
32. What is nonce?
33. What is key distribution center?
34. What is the difference between Rijndael and AES?
35. what are the elements include in the Public-Key Certifications?
36. Define PGP.
37. Define Public Key Management.
38. What are the applications involved in IP Security?
39. What are the IP Security Mechanisms?
40. Define Authentication Header.
41. Define Authentication Data.
42. Define Padding.
43. What are the services provided by the SSL Record Protocol?
44. What are the key features of SET?
45. Define Certification Authority.
46. Define Masquerader.
47. Define Misfeasor.
48. Define Clandestine User.
49. What are the Techniques involved in intrusion?
50. What are the approaches involved in the Intrusion Detection?
51. Define Rule-Based Anomaly detection.
52. Define Trojan Horses.
53. Define Logic Bomb.
54. Define Virus.
55. What are the four phases involved in the Virus?
56. List out the types of Viruses?
57. What are the Characteristics of Firewall?

EXTRA QUESTIONS

1.What are different IT laws for India?  
2. Cryptography vs Steganography vs Data hiding?  
3.   Explain secret splitting and secret sharing.  
4. Compare and contrast Stream Ciphers vs Block Ciphers.  
5. Differentiate between Symmetric Key Algorithms and Asymmetric Key  
Algorithms  
6. What is the difference in DES & AES.  
7. Use of BLOWFISH? Describe Blowfish.  
8. Attacks on DES.  
9. Explain different modes of Operations.  
10. Differentiate between Linear Cryptanalysis and Differential  
Cryptanalysis.  
11. What do you mean by Public Key Algorithms?  
12. What is RSA? Explain Key Generation and Usage.  
13. Explain Elliptic Curve Cryptography.  
14. What is the output of Hash Algorithms  
15. Differentiate between SHA-1 & MD5.  
16. What are the different ways of Key Generation and Distribution?  
17. What is a Digital Certificate?  
18. What is Digital Signature?  
19. What is revocation? When is it required to be done?  
20.  What do you mean by PKI? Explain.  
21. Explain Diffie Hellman Key Exchange.  
22. How is authentication done? Explain One Way Authentication, Mutual  
Authentication?  
23. Explain Neeham Schroeder Protocol.  
24. What is IPSEC? Explain AH and ESP in Tunnel Mode and Transport  
Mode?  
25. What are Security Associations?  
26. Explain SSL?  
27. Describe Handshake Protocol and Record Layer Protocol.  
 28. What is IKE- Internet Key Exchange Protocol?  
29. What is the necessity of Intrusion Detection Systems?  
30. Explain Anomaly Based, Signature Based, Host Based, Network Based  
Systems?  
31.      Explain the OSI security architecture in detail.  
33.     Describe the transposition techniques in detail.  
34.     Explain the Monoalphabetic ciphers in detail with suitable  
example.  
35.     Explain the concept of secret splitting and secret sharing.  
36.     What is the CRT?  
37.     What is Computer Forensics?  
38.     Why do individuals and organizations need to pay attention to  
Computer Forensics?  
39.     What is digital data?  
40.     Why knowledge of Computer Forensics so important?  
41.     What does a Computer Forensics specialist do?  
42.     What should a company do if an incident occurs?  
43.     Explain the concept of industrial espionage through social engineering.  
44.     What are different methods of Industrial Epsionage?  
45.     How can we prevent Industrial Epsionage?  
46.     What are the risk factors due to Industrial Epsionage? Give the impact of Loss.  
47.      Discuss on Internet Scams and some easy ways to protect yourselves.  
48.     What are Investment Scams? What are its different types?  
49.     How E-mail Scams Work? Discuss on how to report and avoid them?  
50.     Spam mail - 'Nigerian fraud 419', Discuss.  
51.     What are Corporate Epsionage Techniques? Which are high risk industries?  
52.     What is phishing scam? How does it work?  
53.     What is the Indian IT Act? Give the Scope and Coverage of the Indian IT Act.  
54.     What is intellectual property Rights (IPR) , Patent Law, Copyright Law  
55.     What are benefits of ISO 27001certification?  
56.     Write a note on Payment types.  
57.     Explain the concept of Mobile Payments.  
58.     What are the possible attacks on the E-Transaction using cards?  
59.     Discuss the issues and concerns for Payment over the Internet.  
60.     Write a note on Electronic Cash.