PART-A Questions

1. Name the aspects to be considered of information security.

2. What is meant by deciphering?

3. What are the two different uses of public key cryptography related to key distribution?

4. How many bit keys are used in S-DES algorithm?

5. Name the processing steps involved in MD5 logic?

6. What are the parameters are include the certificate request message?

7. What is S/MIME?

8. What is the purpose of dual signature?

9. What are the two common techniques used to protect a password file?

10. What are the req1.

11. What is the size of the key for substitution block cipher?

12. Define Stream Cipher.

13. What is convert channel?

14. Give the principle advantages of elliptical curve cryptography.

15. What are the counter measures for timing attach?

16. Give all the generic types of attacks.

17. How secure is DES?

18. What is the necessity of firewalls?

19. Between symmetric Vs Public Key cryptography, which method is more convenient?

20. What are the requirements of a hash function?

21. Security threats can be categorized into ___________ & __________.

22. Two kinds of threats can be presented by programs, they are __________ & __________.

23. It is possible to provide ______ & _____________ by a double use of public key scheme.

24. A public key is denoted as _________ & private key as ______________.

25. In context of communications across a network, the following attacks can be identified __________, __________, ___________ & __________________.

26. Simplest has function can be expressed as __________________.

27. PGP provides a ______________ & ______________ services, that can be used for E-Mail and file storage application.

28. The five header fields defined in MIME are as follows: ____________ ,___________, ___________,____________ & ______________.

29. _____________ & ______________ are the standardized schemes that are becoming increasingly important as part of Web Commerce.

30. SET incorporates the following features ________,_________,_________ & ____________.

31. What are symmetric and asymmetric encryptions?

32. What is the main advantage of AES over DES?

33. What is a nance?

34. What are public and private keys?

35. The addition operation in ECC is the counterpart of modular __________ in RSA and multiple addition is the counterpart of modular _______________.

36. For what purpose the hash function is used?

37. What is Kerberos?

38. Where do you apply PGP?

39. Give application for Class I Veri Sign public key certificate.

40. The intruders are classified into _________, _________ and ---------------.

41. List out different active attacks.

42. Mention the drawback of Steganography.

43. List out the basic tasks in Public Key Encryption in key distribution.

44. Diffie-Hellman algorithm also supports Digital Signature application. Say True or False.

45. _________ provides a Centralized authentication Server whose function is to authenticate users to Servers and Servers to users.

46. Give an example for Simple Hash Function.

47. List out the two methods of operations in Authentication Header (AH) and Encapsulating Security Payload (ESP).

48. Enumerate the functions provided by S/MIME.

49. _________ infects a master boot record boot record and spreads when a system is booted from the disk containing the virus.

50. List out the two ways in which password can be protected.

51. Which attack is related to integrity?

52. Most symmetric block ciphers are based on __________ structure.

53. Which public key cryptosystem can be used for digital signature?

54. In asymmetric key cryptography __________keys are required per user.

55. X .509 standards is used in __________and __________.

56. The length of message digest is __________bits for SHA.

57. Expand: S/MIME.

58. What is the use of trusted system?

59. Give the methods for protecting the password file.

60. First version of TLS can be viewed as __________.

61. Which attack is related to confidentiality?

62. _________ is used to verify the integrity of message.

63. In asymmetric key cryptography _________ keys are required per user.

64. SSL was originated by _________.

65. MAC function is _________ function.

66. The message digest length of MD5 algorithm is _________.

67. PGP finds its use in _________ and _________.

68. List the three different classes of intruders.

69. TLS working group was formed within _________.

70. What is the use of trusted system?

71. Give the four kinds of security threats in the network.

72. Define Cryptanalysis.

73. What is meant by symmetric encryption?

74. Find the ‘n’ and ø(n) value in RSA if P = 7 and Q = 17.

75. Write the specific function of MAC in network security.

76. What type of encryption is used in CMAC authentication?

77. Define Hash function.

78. What are the properties of Digital Signature?

79. What is meant by SSL?

80. What is meant by Firewall?

81. What are the two basic functions used in encryption algorithms?

82. What is Steganography?

83. What is key distribution center?

84. What is the key size for Blowfish?

85. What is message authentication?

86. Define Kerberos.

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

88. Give the application of IP security.

89. What is meant by SET?

90. List the design goals of firewalls.

91. What is Cryptanalysis?

92. Give the classification of active attacks.

93. List out the basic tasks in Public Key Encryption in key distribution.

94. What is Digital Signature?

95. Kerberos provides ________ whose function is to authenticate users to Servers and Servers to users.

96. Give the purpose of Hash Function.

97. List out different header fields defined in MIME.

98. Give different IPSec Services.

99. _______ infects a master boot record boot record and spreads when a system is booted from the disk containing the virus.

100. Classify Intrusion Detection approaches.

101. Define Network security.

102. What is meant by block cipher and stream cipher?

103. What is nonce?

104. What are the possible ways to distribute the public keys?

105. Write the need and mention the size of the hash buffer in SHA-512.

106. Write the features of Whirlpool.

107. What is PGP?

108. List out the functions of S/MIME.

109. What is change cipher spec protocol?

110. What are the key features of SET?

11 1. Two types of passive are attacks are _______ and __________

112. A ________ is one that encrypts a digital data stream one bit or one byte at a time.

113. What is the use of public key encryption scheme?

114. What is an elliptic curve?

115. What is meant by CBC-MAC?

116. DSA means ___________.

117. List any two web security threats.

118. Define IPSec.

119. List any two design goals for a firewall.

120. SMTP means _____________.

121. Define Security Mechanism.

122. Give any two parameters and design choices that determine the actual algorithm of a Feistel cipher?

123. Identify the possible threats for RSA algorithm.

124. List out the general schemes for the distribution of public keys.

125. Is a 128-bit hash function (MD5) unsuitable for HMAC?

126. What are the areas where Kerberos Version 5 addresses the limitation of Version 4?

127. What is S/MIME?

128. Mention the protocols used by IPSec to provide security.

129. How are the passwords stored in password file in UNIX operating system?

130. Which system is used to protect credit card transactions on the internet?

131. Define Security Service.

132. What is meant by Block Cipher?

133. Define Plain Text.

134. What are the three broad categories of applications of Public Key cryptosystems?

135. Which block size and key size are used in the whirlpool Block Cipher?

136. List out any two design objectives of HMAC.

137. What are the fields in the Authentication Header?

138. Why does Encapsulating Security Payload include a padding field?

139. What is the main service of secure socket layer?

140. What is meant by a Secure Electronic Transaction?

PART –B Questions

1. What is the difference between diffusion and confusion?

2. Define confusion.

3. Give the X.509 certificate format.

4. What is meant by intruders?

5. Explain circuit level gateway.

6. What are diffusion and confusion methods?

7. What is the concept of digital certificate?

8. Give some functions of PGP.

9. Define Reference monitor.

10. What are the types of Firewall

11. Define Streams Cipher.

12. What is purpose of Diffie-Hellman Algorithm?

13. What are the requirements for Kerberos.

14. What are the functions provided by S/MIME?

15. Why we need Trusted System?

16. What is the difference between stream cipher and block cipher?

17. What are the two types of curves used in ECC?

18. What is HMAC and what are its advantages over MAC?

19. What is the main advantage of S/MIME over PGP?

20. List the type of firewall

21. What do you mean by computationally secure encryption?

22. Analyze the characteristic of two keys in Public-Key algorithms.

23. Give the design objectives for HMAC.

24. Analyze the PGP Message Format and its different components.

25. Analyze the attacks on Packet Filtering Firewall.

26. Define: Confusion and Diffusion.

27. List the applications of Public-Key Cryptosystems.

28. Give the requirements that must be met by authentication.

29. Why is PGP popular?

30. Write notes on SET Services.

31. List the type of attacks possible on encrypted messages.
32. Give the steps of Diffie-Hellman key exchange algorithm.
33. Define 3 different approaches to Message Authentication.
34. List the S/MIME Functions.
35. Enumerate the properties of the Reference Monitor.
36. What is AES cipher?
37. What is ECC?
38. What is E-Mail security?
39. List the benefits of IP Security.
40. List the firewall limitations.
41. What is the difference between a block cipher and a stream cipher?
42. List four general categories of schemes for the distribution of public keys.
43. Differentiate MAC and Hash function.
44. What do you mean by Security Association? Specify the parameters that identify the Security Association.
45. List four techniques used by firewalls to control access and enforce a security policy.
46. Give the security strength of Playfair Cipher.
47. Mention the characteristic of two keys in Public-Key security algorithms.
48. Analyze the properties of Hash Function.
49. Compare Transport mode and Tunnel Mode.
50. Write short notes on Viruses.
51. What is diffusion and confusion?
52. Distinguish between symmetric and asymmetric encryption techniques.
53. Discuss the requirements of Kerberos.
54. List out any three benefits of IPSec.
55. What are the design goals of firewall?

56. What is the strength of DES?

57. What is the zero point of an elliptic curve?

58. List the process steps of SHA.

59. What are the header fields defined in MIME?

60. List the key features of SET.

61. Distinguish between Block and Stream Ciphers.

62. Summarize trap-door one-way function.

63. Give the general format of X.509 certificate.

64. Why does ESP include a padding field?

65. What is Virus? Mention its types

66. Write short note on elliptic Curve cryptography.

67. What is meant by Kerberos?

68. What are the five principal services provided by PGP?

69. What are the different four techniques used to avoid guessable passwords?

70. List and explain in different types of Security Attacks.

PART-C Questions

1. Explain the encryption and decryption techniques of classical Feistel network.

2. Explain the substitution bytes transformation and add round key transformation of AES cipher.

3. Explain in detail the Diffie Hellman key exchange algorithm.

4. Discuss the elliptic curve cryptography.

5. Explain the SHA-1 processing of a single 512-bit block and also give the single step operation.

6. Briefly explain the Kerberos version 4 messages exchanges and give the over view of Kerberos using a diagram.

7. a. What are the five principal services provided by pretty good privacy?

b.Why does pretty good privacy generate a signature before applying compression?

8 Write short notes on S/MIME.

9. Discuss the basic techniques of password selection strategies.

10. Explain the trusted systems.

11. Explain the structure of Fiestel Cipher with an example.

12. Give short notes on AES Cipher.

13. Give notes on Diffi-Hellman key exchange.

14. Give short notes on RSA algorithm. Encrypt the message “This is encrypted text” using the values p = 7 and q = 17.

15. Explain MD5 hashing function with an example.

16. How does a client C communicate with a server S using Kerberos protocol? Explain.

17. Person A wants to send a confidential email M to person B. How can it be sent?

18. Describe about IP security.

19. How a password can be protected in UNIX? Give some other method for protecting the password.

20. Give short notes on SSL handshake protocol.

21. a.Explain in detail Kerberos version 5 authentication dialogue.

b. Discuss about Secure Hash Algorithm (SHA)

22. a. Explain the Key generation process in Data Encryption Standard (DES)

algorithm.

b.Describe the AES Key Expansion Algorithm .

23. a.Discuss in detail about active and passive attacks.
b.Describe the DES encryption process and the strength of DES.

24. a. Discuss about Elliptic Curve Cryptography.
b. What is meet-in-the-middle attack?
c. List few requirements for public key cryptography.

25. a Explain RSA algorithm. Throw some light on the security of RSA.
b. Discuss Diffie Hellman Key Exchange algorithm .

26. a. Write short notes on IP security architecture.
b. Give an overview on S/MIME functionality.

27. a. Write short notes on Pretty Good Privacy.
b. Describe Encapsulating Security Payload (ESP) format.

28. a. Discuss about different types of firewall.
b.Give the architecture for Distributed Intrusion Detection and explain.

29. a. Discuss in detail about Secure Electronic Transaction.
b. Give the architecture of Digital Immune System and explain.

30. a. Explain with a neat sketch about the DES modes of operation.
b. Write down the composition of functions for simplified DES

31. a. Draw the diagrams for various security attacks.
b. With the help of a diagram explain the details of single round in DES

32. a. Draw the public key distribution scenario.
b. Perform encryption & decryption using RSA algorithm.
c. Differentiate between Conventional & Public key Encryption algorithms

33. a. What is the characteristic of public key cryptosystem?
b. With a neat sketch explain public key cryptography for secure and authentication.
c. Write down the Diffie-Hellman key exchange Algorithm.

34. a.With a neat sketch explain the Authentication procedure of X.509.
b.What is an environmental short coming?

35. a.Give examples of replay attacks.
b.Draw the sketch of HMAC.

36. a.Sketch the IPSec Document Overview diagram.
b.What are all the Cryptographic algorithm used in S/MIME.
c.Draw the PGP Cryptographic function for Authentication only.

37. a.Draw the General format of PGP Message.
b.With neat sketch explain IPSec Authentication Header.

38. a.Write down the chart that shows the comparison of threats on Web
b.With a neat diagram explain the operation of SSL Record Protocol.
c.Write short notes on Types of Firewalls.

39. a.How Security facilities are located in TCP/IP protocol stack for Network layer,

Transport layer and Application Layer.

b.With a neat diagram explain Card holder – Purchase Request Operation in SET.

40. Draw the block diagram of simple DES and explain the S-DES algorithm.

41. Explain the encryption and decryption techniques for AES with neat diagrams.

42. a. Explain the different methods of public key distribution systems with suitable diagrams.

    b. Also explain the Diffie – Hellman algorithm.

43. a. List the requirements for public key cryptography.

    b. Explain the RSA algorithm with suitable example.

44. Explain the MD5 message digest algorithm by giving suitable diagrams for message digest generation and message processing of 512 bit block and MD5 operation.

45. a. What are the two types of digital signature? Explain each briefly. Also explain the digital signature algorithm and the digital signature system.

    b. Compare MD5 with SHA – 1

46. a. What is PGP? How authentication and confidentiality is maintained in PGP.

    b.Explain the keyrings and its significance in PGP. Also explain the message generation from sender to receiver with suitable diagram.

47. a.Draw the IP security authentication header and explain the functions of each field.

    b. What are transport mode and tunnel mode authentication in IP? Explain. How ESP is applied to both these modes?

48. What is SET?. Explain how Secure Electronic Transaction is used for E- Banking with suitable block diagrams in terms of card holders purchase request and verification by the merchants.

49. What are the characteristic requirements for firewall? Explain the types of firewalls and possible attacks and the related counter measures.

50. a.Explain the different methods of public key distribution with suitable diagrams and show how secret keys are exchanged using public keys

    b. With suitable example explain the DIFFIE – HELLMAN algorithm.

51. Draw the general structure of simple DES and explain how encryption and decryption are carried out. Also mention the strength and weakness of DES algorithm.

52. a. Explain the AES method of encryption and decryption.

b. Explain the RC4 stream cipher method used for encryption and decryption.

53. Explain the SHA algorithm by giving suitable diagrams.

54. a. Explain the digital signature and how it is used for authentication? Explain by giving specific application.

b. What are Kerberos? Explain. Also explain the X.509 authentication service.

55. How does PGP provide authentication and confidentiality for e-mail services and for file transfer applications? Draw the block diagram and explain the components.

56. What are the important factors of security in IP networks? Explain the Transport mode and Tunnel mode of security mechanisms in IP security by appending ESP into the Tunnel mode.

57. a. Explain the Secured Socket Layer (SSL) and Transport Layer Security (TSL) in detail.

b. What is Intrusion? How it is detected? Explain the methods of Intrusion detection.

58. a. Explain the Firewall design principles.

b. What are viruses? Explain the virus related threats and the counter measures applied.

59. Explain about the security attacks and its service mechanism.

60. Discuss the AES cipher in detail.

61. Discuss RSA with computations for public key cryptography. Also perform the Encryption and decryption for p =7 , q = 11, e = 17 and m = 8

62. Describe the services provided by X.509 authentication service.

63. What is meant by message digest and discuss about HMAC digital signatures.

64. Explain about the authentication header of IP.

65. Discuss about encapsulating security payload of IP.

66. a.Define intrusion detection and explain the different types of detection mechanisms in

detail.

b.Write short notes on Password selection strategies and their significance.

67. Explain the types of firewalls in detail.

68. a Explain simplified DES with example.

b. How AES is used for encryption/decryption? Discuss with example.

69. a. Explain the various modes of operation?

b. Briefly explain the idea behind Elliptic Curve Cryptosystem.

70. a. Explain Diffie Hellmann key Exchange in detail with an example.

b. Explain RSA algorithm in detail with an example.

71. a. Describe HMAC algorithm in detail.

b. Assume a client C wants to communicate with a server S using Kerberos protocol. How can it be achieved?

72. a. Write and explain the Digital Signature Algorithm.

b. Explain Kerberos in detail.

73. a. Explain the operational description of PGP.

b. Write Short notes on S/MIME.

74. a. Explain the architecture of IP Security.

b. Write short notes on authentication header and ESP.

75. a. Explain Secure Electronic transaction with neat diagram.

b. Write short notes on Intrusion Detection.

76. a. Explain Firewalls in detail.

b. Define virus. Explain in detail.

77. a. Explain about PGP services and it security options.

b. Summarize the S/ MIME capabilities.

78. a. Explain Classical Encryption Techniques.

b. Briefly describe about the strength of DES.

79. a. Explain the Block Cipher principles.

b. Discuss about the AES Cipher and its evaluation criteria.

80. a. Describe about Traffic Confidentiality.

b. Describe Public Key Cryptography.

81. a. Describe Diffie-Hellman Key Exchange.

b. Explain RSA algorithm.

82. a. Explain Authentication Functions.

b. Describe HMAC algorithm.

83. a. Briefly describe about the Secure Hash Algorithm.

b. Explain Digital Signature Standard.

84. a. State and explain Password Management.

b. Explain the Firewall Design Principles.

85. a. Explain briefly about the trusted systems.

b. Explain Intrusion Detection and its approaches.

86. Explain Feistel Cipher Structure and analyse its design principles.

87. a. Analyze the Timing Attacks in DES.

b. Describe about Advanced Encryption Standard (AES) in detail.

88. Explain RSA Algorithm and analyze its Key Generation and Security with an example.

89. a. Compare RSA, Diffie – Hellman, Digital Signature Standard and Elliptive Curve Cryptography algorithms in terms of encryption / decryption, Digital Signature, Key exchange.

b. Analyse the Security of Public Key Schemes.

90. Analyze the three different Authentication Procedures in X.509 Certificate.

91. Analyze MD5 Message Digest Algorithm in detail.

92. Analyze how PGP provides confidentiality and authentication services to electronic mail application.

93. Explain IP Security and analyze its architecture in detail.

94. Analyze the components of Secure Electronic Transactions (SET) and how is SET carried out. Explain.

95. Explain the operation of the following in detail.

a. Viruses

b. Worms

96. Write detailed notes on security services, mechanisms and attacks.

97. Describe the working of AES cipher with neat sketches.

98. Explain the following:

a. Principles of Public key cryptosystem and its applications.

b. Requirements of Public key cryptography.

99. a. Explain RSA algorithm with an example.

b. Describe the steps of Diffie-Hellman key exchange algorithm.

100. Describe about SHA algorithm and compare its features with MD5.

101. Explain X.509 authentication service with relevant diagrams.

102. a. Give the frame format of IPSec authentication header and explain.

b. Describe the ISAKMP format with diagrams.

103. Explain how the messages are generated and received by PGP.

104. Describe about

a. Firewall characteristics.

b. Types of firewalls

105. Discuss about SSL architecture and SSL record protocol.

106. a. Explain the Advanced Encryption Standard method of encryption and decryption.

b. Explain how the RC4 stream cipher is used for encryption and decryption.

107 . Explain the simple DES with suitable diagram and explain how encryption and decryption are carried out. What are the major strength and weakness of DES algorithm?

108 . a. What is a public key and a private key? Explain the different methods of public key distribution with suitable diagram and show how secret keys are exchanged using public keys.

b. With suitable example explain the DIFFIEE – HELLMAN algorithm.

109 . a. Explain the digital signature and how it used for authentication? Explain by giving specific application.

b. Explain Kerberos. What are authentication certificates? Explain the X.509 authentication service.

110. With suitable diagrams explain the SHA algorithm.

111. What is the need for security in IP networks? Explain the Transport mode and Tunnel mode of security mechanisms in IP security by appending ESP into the Tunnel mode.

112. Draw the diagrams to show how PGP provides authentication and confidentiality for email services and for the transfer applications.

113. What are viruses? Explain the virus related threats and the counter measures applied. What is firewall and how does it protects the systems?

114. What is Intrusion? How is it detected? Explain the methods of Intrusion detection. Also explain the Secured Socket Layer (SSL) and Transport Security Layer (TSL) in detail.

115. a. Explain the block cipher modes of operation.

b. Briefly describe the strength of DES.

116. How is Feistel cipher used in AES? Explain.

117. Explain about the Diffie –Hellman key exchange.

118. Explain the Principle behind the digital signature standard.

119. Discuss the Kerberos version-5.

120. Explain about S/MIME in detail.

121. a. What are the services provided by PGP? Explain.

b. With neat sketch explain the IP security architecture.

122. Discuss about viruses and threats related to it.

123. Explain about trusted system and common criteria for information technology security.

124. Explain the working of AES cipher with neat sketches.

125. Discuss in detail about DES encryption and decryption algorithms.

126. Explain RSA algorithm with an example and test for primality. Also list the possible attacks on it.

127. Explain the following:

a. Principles of Public key cryptosystem and its applications.

b. key cryptography.

128 . Explain X.509 authentication service with relevant diagrams.

129. With relevant diagrams explain HMAC algorithm and give its strengths.

130. Give the operational description of PGP in detail.

131 . Explain the implementation of IP security architecture in detail.

132 . Describe the following:

SET operation, SET features, Dual signature and payment processing.

133. a. Enumerate the need for using firewalls to provide system security.
b. Discuss about the types of firewalls.

134. Discuss in detail about Data Encryption Standard and its strength.

135. a. Explain in detail about any two transformations in AES encryption procedure.
b. List and briefly define categories of passive and active security attacks.

136. Discuss in detail about RSA algorithm with example. Discuss about its computational aspects for various operations.

137. a. Discuss in detail about Diffie Hellman key exchange algorithm with example.

b. Write in brief about the various modes of operation of block cipher.

138. Sketch the X.509 formats and explain the fields. Explain about authentication procedures supported in X.509.

139. Give a detailed description on Whirlpool and its performance.

140. How does IPSec ESP provide transport and tunnel mode operation? Explain with neat sketch.

141. Explain in detail about firewalls, characteristics and types with needed block diagrams.

142. Sketch the SSL Record format and describe about the services and protocols comprised in SSL Record protocol.

143. Write a detailed note on stream ciphers and block ciphers.

144. Explain the various types of cryptanalytic attacks.

145. Discuss in detail about Prime Factorisation.

146. Discuss in detail about RSA public key encryption.

147. Explain in detail about MAC algorithms and its requirement.

148. With example, explain the Kerberos in detail.

149. Explain IP security architecture using a neat diagram.

150. Discuss in detail about Encapsulating security payload.

151. Explain about secure socket layer architecture and its needs.

152. Discuss in detail about Intrusion detection and Trojan Horse Defense.

153. Explain AES Encryption and Decryption Techniques.

154. a. Discuss Traffic Confidentiality in detail.

b. Explain RC4 algorithm in detail.

155 . a. Users A and B use the Diffie-Hellman key exchange technique a common prime q=71 and a primitive root a=7.

i) If user A has Private Key XA=5, what is A's Public key YA?

ii) If user B has Private Key XB=12, what is B's Public key YA?

iii) What is the Shared secret key?

b. Explain the Security of RSA Algorithm.

156. a. Explain in detail about the requirements for Hash functions.

b. Explain in detail about SHA-512 Logic.

157. Explain in detail about Mutual Authentication protocol.

158. a. Explain Pretty Good privacy in detail.

b. Write short notes on:

i) S/MIME

ii) Kerberos

159. a. Explain IP Security Architecture.

b. Explain Encapsulating Security Payload.

160. a. What protocols comprise SSL? Explain.

b. Explain Statistical Anomaly Detection in detail.

161. a. Explain about Trusted system in detail.

b. Explain Viruses and related threats in detail.

162. Explain Data Encryption Standard in detail.

163. a. Briefly explain the evaluation criteria of AES.

b. Explain with neat diagram AES Key Expansion.

164. a. Explain Diffie Hellman key Exchange in detail with an example.

b. Perform Encryption and decryption for p =7, q = 11, e = 13 and m = 2 using RSA.

165. Discuss in detail about RC4 Cipher.

166. Explain in detail X.509 Authentication Service.

167. Describe in detail the services provided by Pretty Good Privacy.

168. Briefly explain Authentication Header and Encapsulating Security Payload in IP Security.

169. Explain in detail Secure Electronic Transaction.

170. Discuss the different types of firewall and its configurations.

171. a. Discuss any two substitution cipher encryption methods.

b. Explain briefly about Strength of data encryption standard.

172. Explain the OSI Architecture.

173. Describe Diffie-Hellman Key Exchange.

174. Perform encryption and decryption using the RSA algorithm for the following:

a. p = 3; q = 11, e = 7; M = 5

b. p = 5; q = 11, e = 3; M = 9

Hint: Decryption is not as hard as you think; use some finesse.

175. Explain X.509 Authentication Services. Explain Secure Hash Algorithm.

176. a. Summarize the S/MIME capabilities.

b. What are the services provided by IPSec?

177. Discuss about PGP services and it security options.

178. Explain the Firewall Design Principles and its types.

179. Discuss about Intrusion Detection and approaches of Intrusion Detection.

180. a. Explain different types of Cryptanalytic Attacks.

b. Explain Feistel Cipher Structure and analyse its design principles.

181. Analyze the strength of DES Algorithm.

182. a. Analyze the Security of Public Key Schemes.

b. Explain RSA Algorithm and analyze its Key Generation and Security.

183. Explain diffie-hellman key exchange algorithm with an example.

184. a. Analyze the design objectives for HMAC.

b. Explain different Authentication Procedures in X.509 Certificate.

185. a. Describe about the properties of Digital Signature Standard.

b. Analyze MD5 Message Digest Algorithm in Detail.

186. a. Give the PGP Message Format and analyze its components.

b. Analyze the role of Authentication Header and its Structure.

187. Explain IP Security Architecture in detail.

188. Explain the Components of Secure Electronic Transaction (SET) and analyze how SET Transactions carries out.

189. a. Describe the architecture of SSL and related Protocols.

b. Explain different types of Firewalls and their Configuration

190. Explain the encryption and decryption techniques in DES.

191. a. Draw the AES encryption and decryption general diagram.

b. Discuss the overall comments about AES structure.

192. Summarize the RSA algorithm and perform encryption and decryption using RSA Algorithm:

$$p = 3;\ q = 11;\ M = 5$$

193. Explain the Diffie-Hellman Key Exchange with one example.

194. Explain Digital Signature Standard.

195. Briefly discuss the overview of Kerberos and explain the Kerberos version 4 a Simple Authentication Dialogue and More Secure Authentication Dialogue.

196 . Explain the following PGP services:

a. Authentication and Confidentiality
b. Compression
c. E-Mail Compatibility
d. Segmentation

197. Explain the IP Security Architecture in detail.

198. Explain the various types of intrusion detection approaches.

199. Explain the different types of firewalls with neat diagrams.

200. Bring out the differences between Block cipher and Stream cipher. Explain in detail.

201. Discuss in detail the final set of criteria used by NIST to evaluate AES candidate?

202. What are the principle elements of a public key cryptosystem? Explain them.

203. Explain the RSA algorithm with a suitable example.

204. Describe in detail the overall operation of HMAC algorithm.

205. Discuss about the overview of Kerberos in detail.

206. With a neat diagram explain about the IP security architecture.

207. a. Enumerate the differences between transport mode and tunnel mode?

b. What are the symbols used in pretty good privacy? Explain in detail.

208. a. Discuss about the SSL architecture.

b. Briefly explain the statistical anomaly detection technique.

209. Discuss the firewall design principles in detail.

210. a. Explain about PGP services.

b. Describe S/MIME.

211. a. Explain the OSI Architecture.
b. Explain Classical Encryption Techniques.

212. a. Explain DES and AES Algorithm.

b. Describe about Traffic Confidentiality.

213. a. Describe Diffie-Hellman Key Exchange.

b. Explain RSA algorithm and state approaches for attacking RSA algorithm and the counter measures for the same.

214. a. Describe Public Key Cryptography.

b. Explain Elliptic Curve arithmetic.

215. a. Explain Authentication Functions.

b. Describe HMAC algorithm.

216. a. Explain any one of approach and algorithm for Digital Signatures.

b. Explain Authentication protocols.

217. a. Explain Intrusion Detection.

b. State and Explain Password Management and password selection strategies.

218. a. Explain the Firewall Design Principles.

b. Describe about Trusted Systems.

219. With a neat sketch, explain about the DES encryption and decryption process with the internal structure of a single round of DES algorithm.

220. a. In AES, how is the encryption key expanded to produce keys for the 10 rounds?

b. Discuss about the evaluation criteria of AES used by NSIT.

221. Summarize RSA Algorithm. Perform Key Generation for the prime numbers 17 and 11 and perform Encryption and Decryption for the plaintext input of 88.

222.a. Users A and B want to establish a secret key using Diffie-Hellman key exchange protocol using a common prime q= 353, a primitive root α= 3, A's secret key X_A=97 and B's secret key X_B=233. Compute

i. A's public key, Y_A

ii. B's public key, Y_B

iii. A's and B's common secret key, K

b. Using elliptic curve cryptography, explain how secret keys are exchanged and messages are encrypted.

223. a. Briefly describe about the overall processing of Message Digest Generation using MD5 with necessary block diagram.

b. Compare the features of MD5, SHA-1 and RIPEMD-160 algorithm.

224. Write down the Digital Signature Algorithm (DSA) and also show how signing and verification of digital signatures is done using DSS with the block diagrams.

225. What is PGP? What are the principal services provided by PGP? Illustrate each PGP service with a neat diagram.

226.a. With a neat diagram, briefly explain about IPSec Authentication Header (AH) and Anti-Replay mechanism in IPSec.

b. Give an overview of Oakley Key Determination Protocol.

227. What are the services provided by the SSL Record Protocol for SSL connections? Explain the operations performed by the SSL Record Protocol?

228. a. Suggest any three password selection strategies and identify their advantage and disadvantages if any.

b. What kind of attacks is possible on packet filtering firewalls and suggest appropriate counter measures.

229. Explain in detail about the Data Encryption Standard.

230. Discuss in detail about the AES cipher.

231. Explain in detail about the RSA algorithm.

232. Briefly explain about the Diffie-Hellman Key Exchange.

233. Explain in detail about the Secure Hash Algorithm.

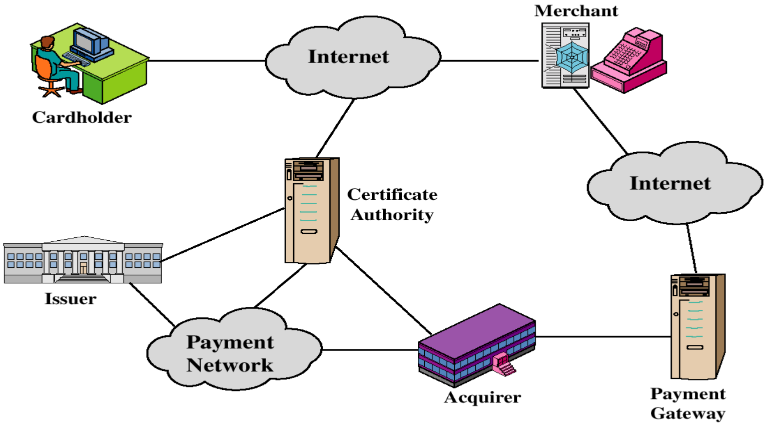
234. Discuss in detail about the Digital Signature Standard.

235. Explain in detail about the S/MIME.

236. Explain in detail about the IP Security Architecture.

237. Discuss in detail about the Distributed Intrusion Detection.

238. Briefly explain in detail about the Firewall Design.


Merchant
Cardholder
Internet
Internet
Certificate Authority
Issuer
Payment Network
Acquirer
Payment Gateway