

101. In Elgamal cryptosystem, given the prime  $p=31$ , What is the respective plaintext character for  $C = (27, 20)$ ?

- A. h
- B. l
- C. o
- D. m

Answer» A. h

[discuss](#)

[discuss](#)

102. How many real and imaginary roots does the equation  $y^2=x^3-1$  have?

- A. 2 real, 1 imaginary
- B. all real
- C. all imaginary
- D. 2 imaginary, 1 real

Answer» D. 2 imaginary, 1 real

103. “In ECC, the inverse of point  $P = (x_1, y_1)$  is  $Q = (-x_1, y_1)$ . “

- A. true
- B. false

Answer» B. false

[discuss](#)

104. In the elliptic curve group defined by  $y^2 = x^3 - 17x + 16$  over real numbers, what is  $P + Q$  if  $P = (0, -4)$  and  $Q = (1, 0)$ ?

- A. (15, -56)
- B. (-23, -43)
- C. (69, 26)
- D. (12, -86)

Answer» A. (15, -56)

[discuss](#)

105. How many real and imaginary roots does the equation  $y^2=x^3-4x$  have?

- A. 2 real, 1 imaginary
- B. all real
- C. all imaginary
- D. 2 imaginary, 1 real

Answer» B. all real

[discuss](#)

106. In the elliptic curve group defined by  $y^2 = x^3 - 17x + 16$  over real numbers, what is  $2P$  if  $P = (4, 3.464)$

- A. (12.022, -39.362)
- B. (32.022, 42.249)
- C. (11.694, -43.723)
- D. (43.022, 39.362)

Answer» A. (12.022, -39.362)

[discuss](#)

107. In public key cryptosystem, \_\_\_\_\_ keys are used for encryption and decryption.

- A. same
- B. different
- C. encryption keys
- D. none of the mentioned

Answer» B. different

[discuss](#)

108. PGP system uses \_\_\_\_\_

- A. private key system
- B. public key system
- C. private & public key system
- D. none of the mentioned

Answer» C. private & public key system

[discuss](#)

109. Knapsack problem can be solved by \_\_\_\_\_

- A. public key cryptosystem
- B. public key system
- C. private & public key system
- D. none of the mentioned

Answer» A. public key cryptosystem

[discuss](#)

110. Merkle hellman is a symmetric cryptosystem.

- A. true
- B. false

Answer» B. false

[discuss](#)

111. In public key cryptosystem, \_\_\_\_\_ is kept as public?

- A. encryption keys

111. **In public key cryptosystem which is kept as public?**

- B. decryption keys
- C. encryption & decryption keys
- D. none of the mentioned

Answer» A. encryption keys

[discuss](#)

112. **A cryptographic hash function has variable output length.**

- A. true
- B. false

Answer» B. false

[discuss](#)

113. **In a trapdoor function, the functions are easy to go in**

- A. one direction
- B. two directions
- C. all directions
- D. none of the mentioned

Answer» A. one direction

[discuss](#)

114. **Which algorithm can be used to sign a message?**

- A. public key algorithm
- B. private key algorithm
- C. public & private key algorithm
- D. none of the mentioned

Answer» A. public key algorithm

[discuss](#)

115. **In this Merkle Hellman method same key is used for encryption and decryption.**

- A. true
- B. false

Answer» B. false

[discuss](#)

116. **A set of numbers is called as super increasing if**

- A. each element is greater than previous element
- B. each element greater than sum of all the previous elements
- C. each element greater than the average of all elements
- D. each element lesser than the sum of all the elements

Answer» B. each element greater than sum of all the previous elements

[discuss](#)

117. **There are                    major ways of stealing email information.**

- A. 2
- B. 3
- C. 4
- D. 5

Answer» B. 3

[discuss](#)

118. **Which of them is not a major way of stealing email information?**

- A. stealing cookies
- B. reverse engineering
- C. password phishing
- D. social engineering

Answer» B. reverse engineering

[discuss](#)

119. **is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.**

- A. email security
- B. email hacking
- C. email protection
- D. email safeguarding

Answer» A. email security

[discuss](#)

120. **is a famous technological medium for the spread of malware & problems of spam, & phishing attacks.**

- A. cloud
- B. pen drive
- C. website
- D. email

Answer» D. email

[discuss](#)

121. **Fraudulent email messages are some fake email messages that seem legitimate, which asks for your confidential bank details such as                    details & passwords.**

- A. credit card, antivirus name
- B. credit card, login id
- C. cell phone, antivirus name

121. **Fraudulent email messages are some fake email messages that seem which asks for your confidential bank details such as detail passwords.**

D. car model, account id

Answer» B. credit card, login id

[discuss](#)

122. **Unsolicited Bulk E-mails (UBI) are called**

A. sms

B. mms

C. spam emails

D. malicious emails

Answer» C. spam emails

[discuss](#)

123. **Using email hacking illicit hackers can send & spread virus spam emails.**

A. trojans, redirected malicious urls

B. antivirus, patches

C. cracked software, redirected malicious urls

D. malware, security patches

Answer» A. trojans, redirected malicious urls

[discuss](#)

124. **is the technique used for tricking users to disclose their user passwords through fake pages.**

A. social engineering

B. phishing

C. cookie stealing

D. banner grabbing

Answer» B. phishing

[discuss](#)

125. **Which of them is an example of grabbing email information?**

A. cookie stealing

B. reverse engineering

C. port scanning

D. banner grabbing

Answer» A. cookie stealing

[discuss](#)

126. Which of the following is a non-technical type of intrusion or attack technique?

- A. reverse engineering
- B. malware analysis
- C. social engineering
- D. malware writing

Answer» C. social engineering

[discuss](#)

127. If the data stored in the \_\_\_\_\_ is not encrypted, then after cookie s\_\_\_\_\_ attackers can see information such as username and password stor\_\_\_\_\_ cookie.

- A. memory
- B. quarantine
- C. cookies
- D. hard drive

Answer» C. cookies

[discuss](#)

128. The stored cookie which contains all your personal data about that \_\_\_\_\_ can be stolen away by \_\_\_\_\_ using or trojans.

- A. attackers, malware
- B. hackers, antivirus
- C. penetration testers, malware
- D. penetration testers, virus

Answer» A. attackers, malware

[discuss](#)

129. If a website uses a cookie, or a browser contains the cookie, then ev\_\_\_\_\_ you visit that website, the browser transfers the cookie to that webs\_\_\_\_\_

- A. true
- B. false

Answer» A. true

[discuss](#)

130. Which of them is not a proper method for email security?

- A. use strong password
- B. use email encryption
- C. spam filters and malware scanners
- D. click on unknown links to explore

Answer» D. click on unknown links to explore

[discuss](#)

**131. What are email security services?**

- A. confidentiality
- B. authentication
- C. non-repudiation of origin
- D. all of the above

Answer» D. all of the above

[discuss](#)

**132. PGP security system uses**

- A. public key cryptosystem
- B. private key cryptosystem
- C. public & private key cryptosystem
- D. none of the mentioned

Answer» C. public & private key cryptosystem

[discuss](#)

**133. What is the key size allowed in PGP?**

- A. 1024-1056
- B. 1024-4056
- C. 1024-4096
- D. 1024-2048

Answer» C. 1024-4096

[discuss](#)

**134. Who created PGP?**

- A. phil zimmermann
- B. tim berners-lee
- C. marc andreessen
- D. ken thompson

Answer» A. phil zimmermann

[discuss](#)

**135. What is the PGP stand for?**

- A. permuted gap permission
- B. permuted great privacy
- C. pretty good privacy
- D. none of the mentioned

Answer» C. pretty good privacy

[discuss](#)

**136. PGP makes use of which cryptographic algorithm?**

- A. des

**136. PGP makes use of which cryptographic algorithm?**

- B. aes
- C. rsa
- D. rabin

Answer» C. rsa

[discuss](#)

**137. PGP offers            block ciphers for message encryption?**

- A. triple-des
- B. cast
- C. idea
- D. all of the above

Answer» D. all of the above

[discuss](#)

**138. S/MIME stands for            .**

- A. standard multipurpose internet mail extensions.
- B. secure multipurpose internet mail extensions.
- C. secure multipurpose international mail extensions
- D. standard multipurpose international mail extensions.

Answer» B. secure multipurpose internet mail extensions.

[discuss](#)

**139.    is used for hiding the payment information from the merchant.**

- A. set.
- B. ssl.
- C. shttp
- D. tsp

Answer» A. set.

[discuss](#)

**140. The cryptography algorithms used in S/MIME are .**

- A. idea.
- B. rc4
- C. rsa,des-3
- D. rc5

Answer» C. rsa,des-3

[discuss](#)

**141. In S/MIME,MLA stands for .**

- A. mailing list agent.
- B. multipurpose list agent.
- C. mail lock agent.



141. **In S/MIME,MLA stands for .**

D. message link agen

Answer» A. mailing list agent.

[discuss](#)

142. **Which component is included in IP security?**

A. authentication header (ah)

B. encapsulating security payload (esp)

C. internet key exchange (ike)

D. all of the mentioned

Answer» A. authentication header (ah)

[discuss](#) <sup>(1)</sup>

143. **WPA2 is used for security in**

A. ethernet

B. bluetooth

C. wi-fi

D. email

Answer» C. wi-fi

[discuss](#)

144. **An attempt to make a computer resource unavailable to its intended user is called**

A. denial-of-service attack

B. virus attack

C. worms attack

D. botnet process

Answer» A. denial-of-service attack

[discuss](#)

145. **PGP is used in**

A. browser security

B. email security

C. ftp security

D. wifi security

Answer» B. email security

[discuss](#)

146. **In tunnel mode, IPSec protects the**

A. entire ip packet

B. ip header

C. ip payload

**146. In tunnel mode, IPSec protects the**

D. ip trailer

Answer» A. entire ip packet

[discuss](#)

**147. IPSec is designed to provide security at the**

A. transport layer

B. network layer

C. application layer

D. session layer

Answer» B. network layer

[discuss](#)

**148. Which of the following is not a strong security protocol?**

A. https

B. ssl

C. smtp

D. sftp

Answer» C. smtp

[discuss](#)

**149. SSL primarily focuses on**

A. integrity and authenticity

B. integrity and non-repudiation

C. authenticity and privacy

D. confidentiality and integrity

Answer» A. integrity and authenticity

[discuss](#)

**150. Why did SSL certificate require in HTTP?**

A. for making security weak

B. for making information move faster

C. for encrypted data sent over http protocol

D. for sending and receiving emails unencrypted

Answer» C. for encrypted data sent over http protocol

[discuss](#)

[Previous](#)[1234](#)[Next](#)

Done Studing? Take A Test.