Unit I & II

1. _______ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
a) Network Security
b) Database Security
c) Information Security
d) Physical Securiy

2. From the options below, which of them is not a threat to information security?
a) Disaster
b) Eavesdropping
c) Information leakage
d) **Unchanged default password**.

3. From the options below, which of them is not a vulnerability to information security?
a) **flood**
b) without deleting data, disposal of storage media
c) unchanged default password
d) latest patches and updates not done

4. _____ platforms are used for safety and protection of information in the cloud.
a) Cloud workload protection platforms
b) Cloud security protocols
c) AWS
d) One Drive

5. Which of the following information security technology is used for avoiding browser-based hacking?
a) Anti-malware in browsers
b) **Remote browser access**
c) Adware remover in browsers
d) Incognito mode in a browser

6. _______ technology is used for analyzing and monitoring traffic in network and information flow.
a) Cloud access security brokers (CASBs)
b) Managed detection and response (MDR)
c) Network Security Firewall
d) **Network traffic analysis (NTA)**

7. Compromising confidential information comes under _________
a) Bug
b) Threat
c) Vulnerability
d) Attack

8. Lack of access control policy is a _____________
a) Bug
b) Threat
c) Vulnerability
d) Attack

9. Possible threat to any information cannot be ________________
a) reduced
b) transferred
c) protected
d) ignored

10) In which of the following, a person is constantly followed/chased by another person or group of several peoples?

1. Phishing
2. Bulling
3. **Stalking**
4. Identity theft

11) Which one of the following can be considered as the class of computer threats?

1. **Dos Attack**
2. Phishing
3. Soliciting
4. Both A and C

12) Which of the following is considered as the unsolicited commercial email?

1. Virus
2. Malware
3. **Spam**
4. All of the above

13) Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

1. Malware
2. **Spyware**
3. Adware
4. All of the above

14) _______ is a type of software designed to help the user's computer detect viruses and avoid them.

1. Malware
2. Adware
3. **Antivirus**
4. Both B and C

15) Which one of the following is a type of antivirus program?

1. Quick heal
2. Mcafee
3. Kaspersky
4. **All of the above**

16) It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_______:

1. Antivirus
2. **Firewall**
3. Cookies
4. Malware

17) Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?

1. Piracy
2. Plagiarism
3. Intellectual property rights
4. All of the above

Answer: d

18) Which of the following refers to the violation of the principle if a computer is no more accessible?

1. Access control
2. Confidentiality
3. Availability
4. All of the above

Answer: c

19) Which one of the following refers to the technique used for verifying the integrity of the message?

1. Digital signature
2. Decryption algorithm
3. Protocol
4. **Message Digest**

20) In system hacking, which of the following is the most crucial activity?

1. Information gathering
2. Covering tracks
3. **Cracking passwords**
4. None of the above

21) Which of the following are the types of scanning?

1. **Network, vulnerability, and port scanning**
2. Port, network, and services
3. Client, Server, and network
4. None of the above

22) Which one of the following is actually considered as the first computer virus?

1. Sasser
2. Blaster
3. **Creeper**
4. Both A and C

23) To protect the computer system against the hacker and different kind of viruses, one must always keep _________ on in the computer system.

1. Antivirus
2. **Firewall**
3. Vlc player
4. Script

24) Which of the following can be considered as the elements of cyber security?

1. Application Security
2. Operational Security
3. Network Security
4. **All of the above**

25) Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system?

1. DDos and Derive-by Downloads
2. Malware & Malvertising
3. Phishing and Password attacks
4. **All of the above**

26) Which one of the following is also referred to as malicious software?

1. Maliciousware
2. Badware
3. Ilegalware
4. **Malware**

27) Hackers usually used the computer virus for ______ purpose.

1. To log, monitor each and every user's stroke
2. To gain access the sensitive information like user's Id and Passwords
3. To corrupt the user's data stored in the computer system
4. **All of the above**

28) In the computer networks, the encryption techniques are primarily used for improving the ________

1. **Security**
2. Performance
3. Reliability
4. Longevity

29) Which of the following statements is correct about the firewall?

1. It is a device installed at the boundary of a company to prevent unauthorized physical access.

2. **It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.**
3. It is a kind of wall built to prevent files form damaging the corporate.
4. None of the above.

30) Which of the following type of text is transformed with the help of a cipher algorithm?

1. Transformed text
2. Complex text
3. Scalar text
4. **Plain text**

Answer: d

Explanation: The cipher algorithm is used to create an encrypted message by taking the input as understandable text or "plain text" and obtains unreadable or "cipher text" as output. It is usually used to protect the information while transferring one place to another place.

31) In the CIA Triad, which one of the following is not involved?

1. Availability
2. Confidentiality
3. **Authenticity**
4. Integrity

32) In an any organization, company or firm the policies of information security come under__________

1. **CIA Triad**
2. Confidentiality
3. Authenticity
4. None of the above

33) Why are the factors like Confidentiality, Integrity, Availability, and Authenticity considered as the fundamentals?

1. They help in understanding the hacking process
2. These are the main elements for any security breach
3. **They help to understand the security and its components in a better manner**
4. All of the above

34) In order to ensure the security of the data/ information, we need to ____________ the data:

1. **Encrypt**
2. Decrypt
3. Delete
4. None of the above

35) In general how many key elements constitute the entire security structure?
a) 1
b) 2
c) 3
d) **4**

36. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is “this” referred to here?
a) Confidentiality
b) Non-repudiation
c) CIA Triad
d) Authenticity

37.CIA triad is also known as ________
a) NIC (Non-repudiation, Integrity, Confidentiality)
b**) AIC (Availability, Integrity, Confidentiality**)
c) AIN (Availability, Integrity, Non-repudiation)
d) AIC (Authenticity, Integrity, Confidentiality)

38. When you use the word _____ it means you are protecting your data from getting disclosed.
a) Confidentiality
b) Integrity
c) Authentication
d) Availability
View Answer

39. ______ means the protection of data from modification by unknown users.
a) Confidentiality
b) Integrity
c) Authentication
d) Non-repudiation
View Answer

40. When integrity is lacking in a security system, _________ occurs.
a) Database hacking
b) Data deletion
c) Data tampering
d) Data leakage

41. _______ of information means, only authorised users are capable of accessing the information.
a) Confidentiality
b) Integrity
c) Non-repudiation
d) Availability

42. Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
a) They help understanding hacking better
b) They are key elements to a security breach
c**) They help understands security and its components better**
d) They help to understand the cyber-crime better

43. This helps in identifying the origin of information and authentic user. This referred to here as __________
a) Confidentiality
b) Integrity
c) Authenticity
d) Availability

44. Data ___________ is used to ensure confidentiality.
a) Encryption
b) Locking
c) Deleting
d) Backup

45. Which of these is not a proper method of maintaining confidentiality?
a) Biometric verification
b) ID and password based verification
c) 2-factor authentication
d) **switching off the phone**

46. Data integrity gets compromised when _____ and _____ are taken control off.
a) Access control, file deletion
b) Network, file permission
c) **Access control, file permission**
d) Network, system

.

46. ______ is the latest technology that faces an extra challenge because of CIA paradigm.
a) Big data
b) Database systems
c) Cloud storages
d) Smart dust

47. One common way to maintain data availability is __________
a) Data clustering
b**) Data backup**
c) Data recovery
d) Data Altering
View Answer

48. _________ refers to the weakness in the security system.
A. Threat
B. Vulnerability
C. Control
D. Intrusion

49. 2. An analyst can determine an algorithm with sufficient _____.
A. Money
B. Time
C. Key
D. Computer data storage

50. 4. The purpose of computer security is to prevent ______ from doing the _______.
A. attacks, harm
B. attackers, damage
C. threat, needful
D. employees, interference

50 . When an action attempts to compromises the security of information owned by a firm, it is called____.
A. Computer security

B. Internal security

C. Security attack

D. Threat

51. Transposition is also known as ______.

A. Permutation

B. Combination

C. Variation

D. Binomial variation

52. Substitution is an ______ way of encryption.

A. Unacceptable

B. Acceptable

C. Correct

D. Incorrect

53. ______ is the process of encoding a plain text to cipher text.

A. Decryption

B. Cryptanalysis

C. Cryptosystem

D. Encryption

54. 14. Book Cipher uses ______ numbers is any book.

A. Sequential

B. Random

C. Both random and sequential

D. Odd

55. Which of the following is yet to achieve extensive adoption?

A. AES

B. DES

C. RSA

D. PSA

56. Secret key is another name for __________.

A. Stream encryption

B. Symmetric encryption

C. Asymmetric encryption

D. Block encryption

57. Block transformation does not depend on which of the following?

A. Control information

B. User information

C. Symbol
D. Key

58. A cryptanalyst is confronted by how many situations?
A. Four
B. Three
C. Five
D. Six

59 How many users can use a secret key?
A. Three
B. One
C. Two
D. Four

60. One of the major drawbacks of the symmetric system is _____.
A. Key Distribution
B. Key Diffusion
C. Key Confusion
D. Key Construction

61. Repeat cycles are used in ________.
A. AES and RSA
B. AES and DES
C. DES and RSA
D. RSA and VAN

62. ______ operation provides diffusion.
A. Add Subkey
B. Byte Substitution
C. Shift Row
D. Mix Column

63. Each cycle of AES algorithm consists of _____ steps.
A. Three
B. Four
C. Two
D. Five

64. Procedure for _____ is C = E(k1, D(k2, E(k1,m))).
A. Triple DES
B. Double DES
C. DES
D. RSA

65. Public key system is best used for _____.
A. Key exchange
B. Authentication
C. Key exchange and Authentication
D. Validation

66. Asymmetric encryption offers a procedure that wraps the protected information in _______ package(s).
A. Two
B. Three
C. Four
D. One

67. The property of hiding implementation and other design decisions of a component is called___.
A. Modularity
B. Encapsulation
C. Polymorphism
D. Information Hiding

68. In a ______, the frequency of appearance of letter groups can be used to match up plaintext letters that have been separated in a ciphertext.
A. Digram
B. Columnar Transposition
C. Book Cipher
D. Vernam Cipher

69. Ciphertext depends on _______.
A. Original plaintext message
B. Algorithm
C. Key value
D. A, B and C

70. _____ is a classic example of asymmetric key exchange procedure.
A. Certificate
B. Cryptographic hash function
C. Diffie-Hellman Scheme
D. Digital Signature

71. AES algorithm uses _____ for encryption and decryption.
A. Two keys
B. One key
C. Three keys
D. No keys

72. ________ implies that some portion of a ________ message is altered.
A. Deletion, legitimate
B. Modification, Illegitimate
C. Modification, Legitimate
D. Deletion, Illegitimate

73. The basic encryption of ______ involves an arbitrarily long ______ sequence of numbers that are combined with the plaintext.
A. Book Cipher, Repeating
B. Book Cipher, Non-repeating
C. Vernam Cipher, Repeating
D. Vernam Cipher, Non-repeating

74. When the encryption and decryption keys of an encryption algorithm ______, it is called ______.
A. Come in pairs, Asymmetric
B. Come in pairs, Symmetric
C. Are the same, Asymmetric
D. Are not the same, Asymmetric

75. ________ and ________ refers to the amount of labor needed to encrypt a message.
A. Stream encryption, Block encryption
B. Confusion, Diffusion
C. Symmetric algorithm, Asymmetric algorithm
D. Stream decryption, Block decryption

76. Triple-DES uses keys of _____ in _____ operations.
A. Double DES, Two
B. Double DES, Three
C. AES, Three
D. AES, Two

80. Repetitiveness of _____ algorithm, makes it suitable for ______ on a single-purpose chip.
A. DES, Implementation
B. DES, Processing
C. AES, Implementation
D. AES, Processing

81. The fixed _____ key of _____algorithm gave birth to double and triple DES.
A. 64 bit, DES
B. 56 bit, AES

C. 56 bit, DES
D. 64 bit, AES

82.Which one is DES?

a) Block cipher
b) Bit cipher
c) Stream clipher
d) None of the above

83. Encryption system is?

a) Symmetric key encryption algorithm
b) not an encryption algorithm
c) Asymmetric key encryption algorithm
d) None of the above

84. . An asymmetric-key cipher uses
a)1 Key
b)2 Key
c)3 Key
d)4 Key

85 .Cryptography term is used to transforming messages to make them secure and to prevent from
a) Change
b) Defend
c) Idle
d) Attacks

86. Shift cipher is also referred to as the
a)Caesar cipher
b)cipher text
c)Shift cipher
d)None of the above

87. Which one is the Heart of Data Encryption Standard (DES)?

a) DES function
b)Encryption
c)Rounds
d)Cipher

88. . DES stands for…………………

a)Data Encryption Slots

b) Data Encryption Subscription

c)Data Encryption Standard

d)Data Encryption Solutions

87. 0. Encryption algorithm is used to transforms plaintext into…………………

a)Simple Text
b)Cipher Text
c)Empty Text
d) None of the above

88. 1. What is cipher in Cryptography ?
a) Algorithm for performing encryption

b) Algorithm for performing decryption
c) Encrpted Messages

d) Both algorithm for performing encryption and Decryption and encrypted message

89. 1. How many modes of operation are there in in DES and AES?
a) 4
b) 3
c) 2
d) 5

90. Which one of the following modes of operation in DES is used for operating short data?
a) Cipher Feedback Mode (CFB)
b) Cipher Block chaining (CBC)
c**) Electronic code book (ECB)**
d) Output Feedback Modes (OFB)

91. Which of the following is false for ECB mode of operation
i) The Plain text is broken into blocks of size 128 bytes
ii) Blocks can be swapped, repeated, replaced without recipient noticing
iii) Good for short data
iv) Encryption of each block is done separately using a randomly generated key for each block

a) i) only
b) ii) and iii)

c) i) and iv)
d) i) ii) and iv)

92. . Which of the following statements are true
i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption
ii) The CTR mode does not require an Initialization Vector
iii) The last block in the CBC mode uses an Initialization Vector
iv) In CBC mode repetitions in plaintext do not show up in ciphertext

a) iii)
b) ii) and iv)
c) All the Statements are true
d) i) ii) and iv)

93. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from ___
a) 8-16 bits
b) 8-32 bits
c) 4-16 bits
d) 8-48 bits

94. Which of the following can be classified under advantages and disadvantages of OFB mode?
i) Transmission errors
ii) A bit error in a ciphertext segment
iii) Cannot recover from lost ciphertext segments
iv) Ciphertext or segment loss

a) Advantages: None; Disadvantages: All
b) Advantages: All; Disadvantages: None
c) Advantages: i); Disadvantages: ii) iii) iv)
d) Advantages: i); ii) Disadvantages: iii) iv)

95.In OFB Transmission errors do not propagate: only the current ciphertext is affected, since keys are generated “locally”.
a) True
b) False
96. 9. Which of the following modes does not implement chaining or “dependency on previous stage computations”?
a) CTR, ECB
b) CTR, CFB

c) CFB, OFB
d) ECB, OFB

97. 10. The counter value in CTR modes repeats are a regular interval.
a) True
b) False

98. In the AES-128 algorithm there are mainly __________ similar rounds and _________ round is different from other round.

a. 5 similar rounds having 2 pair ; every alternate
b. 9 ; the last
c. 8 ; the first and last
d. 10 ; no

99. Which of the following modes of operation in DES is used for operating?

a. Cipher Feedback Mode (CFB)
b. Cipher Block chaining (CBC)
c. Electronic code book (ECB)
d. Output Feedback Modes (OFB)

100. When do we compare the AES with DES, which of the following functions from DES does not have an equivalent AES function in cryptography?

a. f function
b. permutation p
c. swapping of halves
d. xor of subkey with function f

101. Which of the following is not a type of symmetric-key cryptography technique?

a. Caesar cipher
b. Data Encryption Standard (DES)
c. Diffie Hellman cipher
d. Playfair cipher

102. Which of the following is not a principle of data security?

a. Data Confidentiality
b. Data Integrity
c. Authentication
d. None of the above

103) Which of the following security attacks is not an active attack?
OR
Which of the following attacks is a passive attack**?**

a. Masquerade
b. Modification of message
c. Denial of service
d. Traffic analysis

104. Which of the following options correctly defines the Brute force attack?

a. Brutally forcing the user to share the useful information like pins and passwords.
b. Trying every possible key to decrypt the message.
c. One entity pretends to be some other entity
d. The message or information is modified before sending it to the receiver.

105. **)** "A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?

a. An integer values
b. A square matrix
c. An array of characters (i.e. a string)
d. All of the above

106. A mechanism used to encrypt and decrypt data.

a. Cryptography
b. Algorithm
c. Data flow
d. None of these

107. To encrypt the plaintext, a cryptographic algorithm works in combination with a key...

a. Word, number, or phrase
b. Special Symbols
c. Function Keys
d. All of these

108.The plaintext encrypts to different cipher text with different keys

a. True
b. False

109. Conventional cryptography also known as ... encryption.

a. asymmetric-key
b. logical-key
c. symmetric-key
d. None of these

110. The Data Encryption Standard (DES) is an example of a ...

a. Conventional cryptosystem
b. Asymmetric cryptosystem
c. Caesar's cryptosystem
d. All of these

111. Public key cryptography is a ... cryptosystem

a. Symmetric
b. Asymmetric
c. Symmetric & Asymmetric both
d. None of these

112) Security Goals of Cryptography are

a. Confidentiality
b. Authenticityn
c. Data integrityn
d. Non-repudiation
e. **All of these**

113. A process of studying cryptographic system is known as Cryptanalysis

a. True
b. False

114. Cipher in cryptography is –

a. Encrypted message
b. Algorithm for performing encryption and decryption
c. Both algorithm for performing encryption and decryption and encrypted message
d. Decrypted message

115. The private key in asymmetric key cryptography is kept by

a. Sender

b. **Receiver**
c. Sender and receiver
d. All the connected devices to the network

116. A key is a value that works with a cryptographic algorithm to produce a specific cipher text**.**

a. **True**
b. False

117. A Public key size and conventional cryptography's secret key size are closely related with one another.

a. True
b. **False**

118. The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

a. The input text is divided into two parts: one being left half and another one being right half.
b. Swapping of the left and right halves are performed after each round.
c. **The plain text is converted into a matrix form first**
d. None of the above

119. Among the following given options, chose the strongest encryption technique?

a. DES (Data Encryption Standard)
b. Double DES
c. Triple DES
d. **AES (Advance Encryption Standard**

120. Consider the following steps,

i. Substitution bytes
ii. Shift Rows
iii. Mix columns
iv. Add round key

The above steps are performed in each round of which of the following ciphers?

a. Rail fence cipher
b. Data Encryption Standard (DES)
c. **Advance Encryption Standard (AES)**

d. None of the above

121. We are provided the plain text “SUN”. You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?

a. UWP
b. NUS
c. WUP
d. QSL

122. Which of the following cannot be chosen as a key in the Caesar cipher?

a. An integer
b. An alphabet (A-Z or a-z)
c. A string
d. None of the above

123. Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?

a. Hill Cipher
b. Playfair cipher
c. Both a and b
d. None of the above

124. **)** Which of the following ciphers is a block cipher?

a. Caesar cipher
b. Vernam cipher
c. Playfair cipher
d. None of the above

125. Which of the following ciphers uses asymmetric key cryptography?

a. Rail Fence Cipher
b. Data Encryption Standard (DES)
c. Diffie Hellman Cipher
d. None of the above

126. **)** Which of the following is a mode of operation for the Block ciphers in cryptography?

a. Electronic Code Book (ECB)
b. Cipher Block Chaining (CBC)
c. Counter (CTR) mode

d. **All of the above**

127.) For which of the following should EBC (Electronic Code Book) process not be used for encryption**?**

a. For large block sizes
b. For fixed block sizes
c. For small block sizes
d. None of the above

128. Transposition cipher involves:

(a) Replacement of blocks of text with other blocks
(b) Replacement of characters of text with other character

(c) Strict row to column replacement
(d) Some permutation on the input text to produce cipher text

129. Which of the following is not type of permutation in P-boxes?
(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation

130. Which of the following is not type of permutation in P-boxes?

(a) Plain permutation
(b) Straight permutation
(c) Expansion permutation
(d) Compression permutation

131. Encryption strength is based on:

(a) Strength of algorithm
(b) Secrecy of key
(c) Length of key
(d) All of the above

132. The input block length in AES is:

(a)	56 bits	(b)	64 bits
(c)	112 bits	(d)	128 bits

133. Cryptology means:

(a) Cryptology+ Cryptodesign

(b) Cryptology Cryptanalysis
(c) Cryptograph itself known as cryptology also
(d) None of the above

134. The codified language can be termed as:
(a) Cleartext (b) Unclear text
(c) Codetext (d) Cipher text

135. Decryption algorithm:
(a) Encrypts input data
(b) Decrypts the encrypted data
(c) Both a and b
(d) None of the above

136. In which of the following cryptography the encryption and decryption keys are different?
a. Public key.
b. Private key.
c. Symmetric key.
d. Asymmetric key.

137. In symmetric key crypto, the key is known as a
a. Public key.
b. Private Key.
c. Symmetric key.
d. Asymmetric key.

138. Stream ciphers are like_______, except that we trade provable security for a relatively small key.
a. Simple substitution cipher.
b. Codebook cipher.
c. Double transposition cipher.
d. One-time pad.

139. A stream cipher takes a key K of n bits in length and stretches it into along ___________.
a. Keystream.
b. Search key.
c. Key length.
d. Public key.

140 . Which of the following function is true for stream cipher?
a. StreamCipher (K) =S.

b. Streamcipher (K) =S.
c. Streamcipher(S) =K.
d. StreamCipher(S) =K.

141. CBC stands for
a. Cipher Block chaining.
b. Code Block chaining.
c. Cipher block chain.
d. Code block chain.

142 . Which of the following is not a block cipher modes?
a. CBC.
b. ECB.
c. MCB.
d. Electronic codebook.

143. In which of the following the encryption and decryption key are same?
a. Symmetric key cryptography.
b. Asymmetric key cryptography.
c. Public key cryptography.
d. Non secret key.

144. The keys used in cryptography are

secret key

private key

public key

**All of them **

145. Cryptography, a word with Greek origins, means
corrupting data
secret writing
open writing
closed writing

146 A transposition cipher reorders (permutes) symbols in a

block of packets

block of slots

block of signals

block of symbols

147. Network Security provides authentication and access control for resources.
TRUE

FALSE

148. The process of verifying the identity of a user.

a.authentication

b.identification

c.validation

d. verification

149. Which of these is a part of network identification?

a.user id

b.password

c. otp

d. fingerprint

150 In asymmetric key cryptography, the private key is kept by __________

a. sender
b. receiver
c. sender and receiver
d. all the connected devices to the network

151. In cryptography, the order of the letters in a message is rearranged by __________

1. **transpositional ciphers**
2. substitution ciphers
3. both
4. quadratic ciphers

152. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

1. TRUE
2. **FALSE**

153. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.
a. random polyalphabetic , plaintext , playfair

b. random polyalphabetic , playfair , vignere
c. **random polyalphabetic , vignere , playfair , plaintext**
d. random polyalphabetic , plaintext , beaufort , playfair

154. Rail Fence Technique is an example of

1. Substitution
2. **Transposition**
3. product cipher
4. ceaser cipher

155. Public key encryption is advantageous over Symmetric key Cryptography because of

1. speed
2. space
3. **key exchange**
4. key length

156. The sub key length at each round of DES is__________

1. 32
2. **56**
3. 48
4. 64

157. Which one is the strong attack mechanism?

1. chosen plaintext attack
2. chosen cipher text
3. **brute force attack**
4. man in the middle attack

158. Interception is an attack on

1. Availability
2. **Confidentiality**
3. integrity
4. authenticity

159. The process of writing the text as rows and read it as columns is known as

1. vernam cipher
2. ceaser cipher
3. **transposition columnar cipher**
4. homophonic substitution cipher

160. Encryption Strength is based on

1. strength of algorithm
2. secrecy of key length of key

3. **all of the above**

161 . GCD(a,b) = GCD(b,a mod b)

1. **TRUE**
2. FALSE
3. Cannot be determined
4. None

162. Vigenere table consists of .....

A **26 rows and 26 columns**

B 26 rows and 1 column

C 1 row and 26 columns

D 27 rows and 27 columns

163. Vigenere cipher is harder to decipher than keyword cipher.

A true

B false

164. What will be the plain text corresponding to cipher text "PROTO" if vigenere cipher is used with keyword as "HELLO"?

A WORLD

B INDIA

C AMERICA

165. In which of the following cipher the plain text and the ciphered text does not have a same number of letters?

A affine cipher

B vigenere cipher

C columnar cipher

D additive cipher

166. Use Caesar’s Cipher to decipher the following: HQFUBSWHG WHAW

a. ABANDONED LOCK

b. **ENCRYPTED TEXT**

c. ABANDONED TEXT

d. ENCRYPTED LOCK

167.

Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

a. True

b.False

c.May be

d.can’ t say

168 On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-

a. abqdnwewuwjphfvrrtrfznsdokvl

b. **abqdvmwuwjphfvvyyrfznydokvl**

c. tbqyrvmwuwjphfvvyyrfznydokvl

d. baiuvmwuwjphfoeiyrfznydokvl

169. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text

a. nlazeiibljji

b. nlazeiibljii

c. olaaeiibljki

d. mlaaeiibljki

170. 1. AES uses a ____________ bit block size and a key size of __________ bits.

a) 128; 128 or 256

b) 64; 128 or 192

c) 256; 128, 192, or 256

d) 128; 128, 192, or 256

171. 2. Like DES, AES also uses Feistel Structure.

a) True

b) False

172. The 4×4 byte matrices in the AES algorithm are called

a) States

b) Words

c) Transitions

d) Permutations

173. In AES the 4×4 bytes matrix key is transformed into a keys of size ___________

a) 32 words
b) 64 words
c) 54 words
d) 44 words

174. Which of the 4 operations are false for each round in the AES algorithm
i) Substitute Bytes
ii) Shift Columns
iii) Mix Rows
iv) XOR Round Key

a) i) only
b) ii) iii) and iv)
c) ii) and iii)
d) only iv)

175 There is an addition of round key before the start of the AES round algorithms.
a) True
b) False

176. How many modes of operation are there in in DES and AES?
a) 4
b) 3
c) 2
d) 5

176. Which one of the following modes of operation in DES is used for operating short data?
a) Cipher Feedback Mode (CFB)
b) Cipher Block chaining (CBC)
c) **Electronic code book (ECB)**
d) Output Feedback Modes (OFB)

177. Which of the following is false for ECB mode of operation
i) The Plain text is broken into blocks of size 128 bytes
ii) Blocks can be swapped, repeated, replaced without recipient noticing
iii) Good for short data
iv) Encryption of each block is done separately using a randomly generated key for each block

a) i) only
b) ii) and iii)
c) i) and iv)
d) i) ii) and iv)

178 Which of the following statements are true
i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption
ii) The CTR mode does not require an Initialization Vector
iii) The last block in the CBC mode uses an Initialization Vector
iv) In CBC mode repetitions in plaintext do not show up in ciphertext

a) iii)
b) ii) and iv)
c) All the Statements are true
d) i) ii) and iv)

179. Which of the following modes does not implement chaining or “dependency on previous stage computations”?
a) CTR, ECB
b) CTR, CFB
c) CFB, OFB
d) ECB, OFB

180. The counter value in CTR modes repeats are a regular interval.
a) True
b) False

181. Which of the following modes of operation in DES is used for operating?

a. Cipher Feedback Mode (CFB)
b. Cipher Block chaining (CBC)
c. Electronic code book (ECB)
d. Output Feedback Modes (OFB)

182. _________ is a block cipher.
a. **DES.**
b. IDEA.
c. AES.
d. RSA.

183. DES encrypts data in block size of __________ bits each.
a**. 64.**
b. 128.
c. 32.
d. 56.

184. Data Encryption Standard also called as __________.
a. Data Encryption Algorithm.
b. Double DES.
c. AES.
d. RSA.

185. __________ is generally used in ECB,CBC, or CFB mode.
a. DES
b. AES
c. IDEA
d. RSA.

186. DES consists of __________ rounds to perform the substitution and transposition techniques.
a. 16.
b. 18.
c. 21.
d. 25.

187. _________is the first step in DES.
a. Key transformation.
b. Expansion permutation.
c. S-box substitution.
d. P-box substitution.

188. ___________ substitution is a process that accepts 48 bits from the XOR operation.
a. P-box.
b. **S-box.**
c. Expansion permutations.
d. Key transformation.

189. _________ refers more to asymmetric key cryptography.
a**. Timing attack.**
b. Meet in middle attack.
c. Virus attack.
d. Worms attack
.

190. DES follows
a) Hash Algorithm
b) Caesars Cipher
c) Feistel Cipher Structure
d) SP Networks

191. The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key
a) 12
b) 18
c) 9
d) 16

192. In the DES algorithm the round key is __________ bit and the Round Input is ____________bits.
a) 48, 32
b) 64,32
c) 56, 24
d) 32, 32

193. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via ____________
a) Scaling of the existing bits
b) Duplication of the existing bits
c) Addition of zeros
d) Addition of ones

194. The Initial Permutation table/matrix is of size
a) 16×8
b) 12×8
c) 8×8
d) 4×8

195. The number of unique substitution boxes in DES after the 48 bit XOR operation are
a) 8
b) 4
c) 6
d) 12

196. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
a) True
b) False

197. **DES:**
a. is maintained by ISO
b. refers to Date Electronic Security
c. is a commonly used symmetric encryption algorithm that was developed in the mid-1970s
d. was developed by a joint effort that included Microsoft
e. is an asymmetric algorithm

198. the ________Attack is related to integrity.

a.interception

b.fabrication

c. modification

d. interruption

199. Which of the following is a form of DoS attack?
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) All of the mentioned

200 Sub-key length at each round of DES is
a. 32 bits
b. 56 bits
c. 64 bits
d. 48 bits

201 Which one of the following is active attack?
e. Masquerade
f. Traffic analysis
g. Eavesdropping
h. Shoulder surfing

202. Which one of the following is passive attack?
a. Masquerade
b. Traffic analysis
c. Replay attack
d. Denial of service

203. Number of keys used in asymmetric key cryptography is
a. 04
b. 02
c. 08
d. 16

204 in the ___________attack , the message contents are modified

a. Passive
b. B. active
c. C. bothe of above
d. D.none of above

205. the principle of ______________ensures that the sender of a message cannot later claim that the message was never sent

a. access control
b. authentication
c. availability
d. non-repudiation.

206. the __________ attack is related to availability

a. interception
b.fabrication
c.modification
d.interruption

207. Number of S - boxes used in the DES algorithm is______

(A) 4
(B) 8
(C) 16
(D) 32

208. The length of the key in one-time pad method is______

(A) Random
(B) Fixed
(C) 64
(D) 56

209. Caesar cipher is represented as______

(A) C = (P+26)mod3
(B) C = (P-3)mod26
(C) C = (P+3)mod3
(D) C = (P+3)mod26

210. Which one of the following is not active attack?

(A) Modification of Messages
(B) Replay attack
(C) Masquerade
(D) Traffic Analysis

211. Which one of the following is not a substitution technique?

(A) Poly alphabetic cipher
(B) Play fair cipher
(C) Rail fence technique
(D) Caesar ciphe

212. What will be the ciphertext for the plaintext message=" THIS" with the following key matrix of play fair cipher?

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

(A)DPSX

(B) PDSX
(C) ZFSX
(D) FZSX

213. How monoalphabetic cipher can be attacked?

(A) Crypt Analysis
(B) Reverse the operations
(C) Masquerade
(D) Timing attack

214. The heart of Data Encryption Standard (DES), is______

(A) Cipher
(B) Rounds
(C) Encryption
(D) DES function

215. DES stands for______

(A) Data Encryption Subscription
(B) Data Encryption Standard
(C) Data Encryption Solutions
(D) Data Encryption System

216. Which technique replaces a character with a different character?

(A) Polyalphabetic substitution based
(B) Transposition-based
(C) Substitution based
(D) Mono alphabetic substitution based

217. Which one is DES?

a) Block cipher
b) Bit cipher
c) Stream clipher
d) None of the above

218. Which one is not a RC5 operation?
a) RC5-CipherText Stealing
b) RC5-Cipher Block Chaining
c) RC5-Cipher Padding
d) RC5 block cipher

219. Which RC5 mode will have the ciphertext longer than the plaintext by at most the size of a single RC5 block?

A. RC5 block cipher

B.RC5-Cipher Block Chaining

C.RC5-Cipher Block Chaining Pad

D.RC5-CipherText Stealing

220. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm.

A.11

B.12

C.8

D.6

221. [(a mod n) + (b mod n)] mod n = (a+b) mod n

A .True

B. False

222. Which one of the following is not a RC5 mode of operation?

A.RC5 block cipher

B.RC5-Cipher Block Chaining

C.RC5-Cipher Padding

D.RC5-CipherText Stealing

223. RC5 encryption uses Right shift and decryption uses Left shift.
a) True
b) False
224. "RC5 uses the Feistel Structure."
a) True
b) False

225. Which of these is not a characteristic of block ciphers?
a) Variable key length / block size / number of rounds
b) Mixed operators, data/key dependent rotation
c) Key independent S-boxes
d) More complex key scheduling

226. **In the DES algorithm the round key is __________ bit and the Round Input is ____________bits.**
a) 48, 32
b) 64,32

c) 56, 24
d) 32, 32

227. **In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via ____________**
a) Scaling of the existing bits
b) Duplication of the existing bits
c) Addition of zeros
d) Addition of ones

228. **7. The Initial Permutation table/matrix is of size**
a) 16×8
b) 12×8
c) 8×8
d) 4×8

229. **The number of unique substitution boxes in DES after the 48 bit XOR operation are**
a) 8
b) 4
c) 6
d) 12
230. **XOR and addition operations take place on bytes of size**
a) 8 bits
b) 16 bits
c) 32 bits
d) 64 bits

231. Which of the following is true for the RC5 algorithm?
i) Has variable number of rounds
ii) Has fixed Key length
iii) High memory Requirements
iv) Uses only primitive computational operations commonly found on microprocessors
a) i) and iv)
b) i) ii) and iv)
c) iv)
d) i) ii) and iii)

232. What are the allowable values of word size in bit for RC5 algorithm?
a) 16, 32
b) 16, 32, 64

c) 8, 16, 32
d) 16, 32, 48

233. The number of rounds in RC5 can range from 0 to _____________
a) 127
b) 63
c) 255
d) 31

234. The standard/nominal version of the RC5-w/r/b has parameters w/r/b as
a) 32/18/16
b) 16/18/16
c) 32/12/16
d) 32/16/18

235. The total number of subkeys t used in the RC5 algorithm is given by the formula (r corresponds to number of rounds)
a) t=2r+4
b) t=2r
c) t=2r-2
d) t=2r+2

236. What is breach of availability?
a) This type of violation involves unauthorized reading of data
b) This violation involves unauthorized modification of data
c) This violation involves unauthorized destruction of data
d) This violation involves unauthorized use of resources

Unit 3.

1. A hash function guarantees integrity of a message. It guarantees that message has not be
A.Replaced.
B.Over view.
C.Changed.
D.Left.

2. MCQ. To check integrity of a message, or document, receiver creates the
A.Tag.
B.Hash Tag.
C.Hyper Text.
D.Finger Print.

3. A digital signature needs a
A.private-key system.
B.shared-key system.
C.public-key system.
d. all of above

4. MCQ. One way to preserve integrity of a document is through use of a
A.Thumb Impression.
B.Finger Print.
C.Biometric.
D.X-Rays.

5. Encryption and decryption provide secrecy, or confidentiality, but not
A.Authentication.
B.Integrity.
C.Keys.
D.Frames.

6. MCQ. Digest created by a hash function is normally called a
A.modification detection code (MDC).
B.message authentication connection.
C.message authentication control.
D.message authentication cipher.

7. MCQ. A sender must not be able to deny sending a message that he or she, in fact, did send, is known as
A.Message Nonrepudiation.
B.Message Integrity.
C.Message Confidentiality.
D.Message Sending.

8. MCQ. To preserve integrity of a document, both document and fingerprint are
A.Important.
B.System.
C.Needed.
D.Not needed.

9. MCQ. When data must arrive at receiver exactly as they were sent, its called
A.Message Confidentiality.
B.Message Integrity.
C.Message Splashing.
D.Message Sending.

10. MCQ. Message digest needs to be
A.public.
B.private.
C.kept secret.
D.None.
Answer C

11. MCQ. In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of
A.512 Bit Blocks.
B.1001 Bit Blocks.
C.1510 Bit Blocks.
D.2020 Bit Blocks.

12. MCQ. Message confidentiality or privacy means that sender and receiver expect
A.Integrity.
B.Confidentiality.
C.Authentication.
D.Nonrepudiation.
Answer B

13. Message must be encrypted at sender site and decrypted at the
A.Sender Site.
B.Site.
C.Receiver site.
D.Conferencing.
Answer C

14. block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.
a. **RSA Algorithm**
Rc5 algorithm
SHA-1 Algorithm
ElGamal Algorithm

15. SHA originally designed by _________ & _________ in 1993
a. IBM & NIST
b. **NIST & NSA**
c. NIST
d. All of them

16. SHA-1 requires ____________ rounds

a. 50
b. 70
c.80
d.120

17. The ElGamal Algorithm provides an alternative to the ___________ for public key encryption

a. Deffie hellman key exchange algorithm
b. RSA Algorithm
c. RC5 Algorithm
d. MD5

18. _________________ is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

a. Diffie Hellman key exchange
b. MD5
c. SHA-1
d. ElGamal arithmetic

19. To develop a variety of Elliptic curve cryptographic schemes which can be used
A) Elliptic curve arithmetic

C) Binary curve

B) Prime curve
D) Cubic equation

20. If three points on an Elliptic curve lie on a straight line then their sum is
A) 0 B) 1 C) 3 D) 6

21. In the definition of an Elliptic curve, a single element denoted by O is called the
A) prime point **C) zero point**

B) abelian point D) elliptic point

22. For Cryptography, the variables and coefficients are usually elements of
A) An infinite group B) An infinite algebraic structure
C) infinite bit size **D) a finite algebraic structure**

23. For RSA (modulus n=pq, where p and q are distinct primes and d is the secret exponent) to work, value of P (plaintext) must be less than value of
A) p B) q **C) n** D) r

24. The ElGamal encryption algorithm can be broken by an attacker who is able to:
A) solve the discrete logarithm problem C) generate large prime numbers

B) perform fast exponentiation D) perform a chosen ciphertext attack

25. SHA developed in __________ by NIST And NSA

a. **1993**
b. 1997
c.1992
d.1990
26. SHA is _______ than MD5
a. faster
b.slower
c. both of above
d. none of above

27. value returned by a hash function is called as_____________
a. message digest
b. hash value
c. **both of above**
d. only a

28. pre-image means ____________________
a. it means given an input and its hash ,it should be hard to find a different input with the same hash.
b.it means it should be hard to find two different inputs of any length that result in the same hash
c. it should be computationally hard to reverse a hash function.
d. all of above

29. MD5 digest have been widely used in the software world to provide __________about integrity of transferred file.
a. assistance
b. **assurance**
c. associative
d. gurantee

30. in _______,collision were found in MD5
a. 2007
b.2005
c.2002
d. 2004

31. SHA-1 uses ____________________ security.
a. Secure socket layer
b. Security secure layer
c. socket secure layer
d. security secure layer

32. qubicfunction of ECC_____________________
a**. y^2=x^3+ax+b**
b. y^4=x^3+ax+b
c. y2=x^2+ax+b
d. y^2=x^3+ax+b

33. ECC uses ______________

a. cryptographic curve
b. **eleptic curve**
c. electric curve
d. eletive curve

34. closure, associativity, identity element,inverse element,commutative property are the properties of ____________________.

a. RSA
b. SHA
c. ECC
d. MD5

35. for al a,b in A ,a*b=b*a is _________________.

a. Identity element
b. Commutative property
c. Inverse element
d. Closure property.

36. __________________ points present in eleptic curve

a. Affline points
b. **Affine points**
c. Affilinic points
d. Affirmative points

37. there are maximum _____________ are allowed in ECC
a. 2
b. 4
c. 3
d. 6

38. RSA achieves ________ way encryption
a. **one**
b. two
c.three
d. no

39.in digital signature , signing refered to as _____________ and public key as the ____________
a. verification key ,signature key
b**.**signature key,signing key
c. signature key,verification key
d. none of above

40 _________________ is nothing but service that verify or checks the integrity of that message.
a. Authorization
b. Authentication
c. Assurance
d. Integrity

41. ________________ is defined the signature generated electronically from the digital computer to ensure the identity of sender and contents of message cannot be modifiedduring transmission process.

a. Electrical signature
b. Digital signature
c. Hash value
d. Private key

42. digital signature is ________________ cryptography
a. symmetric key
b.**asymmetric key**
c. private key
d. none of above

43. RSA is also a stream cipher like Merkel-Hellman.
a) True
b) False

44. For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.
a**) C=80**
b) C=92
c) C=56
d) C=23

45. The MD5 is a message digest algorithm developed by ______.
a. Ron Rivest.
b. WhiteField Diffie.
c. Martin Hellman.
d. Diffie-Hellman.

46. The original message digest algorithm is called as _______.
a. MAC.
b. SHA.
c. MD.
d. DSA.
.

47. MD5 is quite fast and produces ________ message digests.
a. 512 bits.
b. 1024 bits.
c. 128 bits.
d. 64 bits.
.

48. The first step of MD5 is __________.
a. add padding bits to original messsge.
b. adding append length bits.

c. divide the input into 512 bit blocks.
d. compression.

49. In MD5, the process block divides the 512 bits into ________ sub blocks.
a. 16.
b. 24.
c. 32
d. 84.

50. Which financial institutions have a relationship with merchants for processing payment card authorizations and payments?
a. Issuer.
b. Acquirer.
c. Merchant.
d. Dealer.

51. Digital signature envelope is decrypted by using _________.
a. merchant private key.
b. payment's private key.
c. payment public key.
d. merchant's public key.

52. _________ helps in ensuring non-fraudulent transactions on the web.
a**. Certificate authority**
b. Digital authority.
c. Dual authority.
d. Digital signature.

53. ___________are very crucial for success of RSA algorithm.
a. Integers.
b. Prime numbers.
c. Negative number.
d. Fraction.

54. _________ is a block cipher.
a. DES.
b. IDEA.
c. AES.
d. RSA.

55. DES encrypts data in block size of __________ bits each.
a. 32.
b. 128.
c. 64.
d. 56.

56. Merkle and Hellman introduced the concept of ________.
a. meet in middle attack.
b. meet in attack.

c. hijack.
d. virus attacks.
Answer: A.

57. Data Encryption Standard also called as __________.
a. Data Encryption Algorithm.
b. Double DES.
c. AES.
d. RSA.
Answer: A.

58. __________ is generally used in ECB,CBC, or CFB mode.
a. DES
b. AES
c. IDEA
d. RSA.
Answer: A.

59. DES consists of __________ rounds to perform the substitution and transposition techniques.
a. 16.
b. 18.
c. 21.
d. 25.
Answer: A.

60. _________is the first step in DES.
a. Key transformation.
b. Expansion permutation.
c. S-box substitution.
d. P-box substitution.
Answer: A.

61. ___________ substitution is a process that accepts 48 bits from the XOR operation.
a. S-box.
b. P-box.
c. Expansion permutations.
d. Key transformation.
Answer: A.

62. __________ refers more to asymmetric key cryptography.
a. Timing attack.
b. Meet in middle attack.
c. Virus attack.
d. Worms attack.
Answer: A.

63. Eli Biham & Adi Shamir introduced ___________.
a. differential & linear cryptoanalysis.
b. Double DES.
c. DES.
d. RSA.
Answer : A.

64. The encryption of an original message can be done __________.
a. only once.
b. twice.
c. thrice.
d. many times.

65. **The ________ method parties**
A. **Diffie-Hellman**
B. RSA
C. DES
D. AES

66. **One commonly used public-key cryptography method is the**

______ algorithm
A. RSS
B. RAS
C**. RSA**
D. RAA

67. ECB & CBC are____________Cipher
a. block
b.stream
c.field
d. none of above

68. AES has _________different configurations
a. two
b.three
c. four
d. five

69. **_______ is a round cipher uses a 128-bit block of data**
A. AEE
B. AED
C. AER
D. AES

70. One of the major drawbacks of the symmetric system is _____.
A. Key Distribution

B. Key Diffusion
C. Key Confusion
D. Key Construction

71. Repeat cycles are used in ________.
A. AES and RSA
B. AES and DES
C. DES and RSA
D. RSA and VAN

72. ______ operation provides diffusion.
A. Add Subkey
B. Byte Substitution
C. Shift Row
D. Mix Column

73. Each cycle of AES algorithm consists of _____ steps.
A. Three
B. Four
C. Two
D. Five

74 Public key system is best used for _____.
A. Key exchange
B. Authentication
C. Key exchange and Authentication
D. Validation

75. Asymmetric encryption offers a procedure that wraps the protected information in _______ package(s).
A. Two
B. Three
C. Four
D. One

76. The property of hiding implementation and other design decisions of a component is called___.
A. Modularity
B. Encapsulation
C. Polymorphism
D. Information Hiding

78 _____ is a classic example of asymmetric key exchange procedure.
A. Certificate
B. Cryptographic hash function
C. Diffie-Hellman Scheme
D. Digital Signature

79. AES algorithm uses _____ for encryption and decryption.
A. Two keys
B. One key
C. Three keys
D. No keys

80. Repetitiveness of _____ algorithm, makes it suitable for ______ on a single-purpose chip.
A. DES, Implementation
B. DES, Processing
C. AES, Implementation
D. AES, Processing

81. The fixed _____ key of _____algorithm gave birth to double and triple DES.
A. 64 bit, DES
B. 56 bit, AES
C. 56 bit, DES
D. 64 bit, AES

82. _____ is a mark made by a sender and recognized easily by the receiver as belonging to the_______.
A. Digital signature, Sender
B. Digital protocol, Sender
C. Electronic signal, Service provider
D. Encrypted key, Message

83. RSA is an _____which does not differentiate between the function of public and private keys of____.
A. Exponential decipher, Users
B. Logarithmic cypher, Senders
C. Exponential cypher, Users
D. Logarithmic decipher, Senders

84. In Deffie-Hellman scheme, each user selects a _______ and computes a ______.
A. Public key, Private key
B. Private key, Public key
C. Public key, Public key
D. Private key, Private key

85. Certificates are built on ____ levels of trust and users decide whether or not to ____ the CA.
A. Changing, Modify
B. Constant, Modify
C. Constant, Trust
D. Changing, Trust

86. If the system is exposed to _______during execution, then _______ are vulnerability.
A. Modification, Trapdoors
B. Testing, Trapdoors
C. Users, Trapdoors
D. Customers, Trapdoors