1. In computer security, ……………………. means that computer system assets can be modified only by authorized parities.

A) Confidentiality

**B) Integrity**

C) Availability

D) Authenticity

2. In computer security, …………………….. means that the information in a computer system only be accessible for reading by authorized parities.

**A) Confidentiality**

B) Integrity

C) Availability

D) Authenticity

3. The type of threats on the security of a computer system or network are ……………………..

i) Interruption                   ii) Interception                  iii) Modification

iv) Creation                         v) Fabrication

A) i, ii, iii and iv only

B) ii, iii, iv and v only

**C) i, ii, iii and v only**

D) All i, ii, iii, iv and v

4. Which of the following is independent malicious program that need not any host program?

A) Trap doors

B) Trojan horse

C) Virus

**D) Worm**

5. The ……….. is code that recognizes some special sequence of input or is triggered by being run from a certain user ID of by unlikely sequence of events.

**A) Trap doors**

B) Trojan horse

C) Logic Bomb

D) Virus

6. The …………….. is code embedded in some legitimate program that is set to “explode” when certain conditions are met.

A) Trap doors

B) Trojan horse

**C) Logic Bomb**

D) Virus

7. Which of the following malicious program do not replicate automatically?

**A) Trojan Horse**

B) Virus

C) Worm

D) Zombie

8. …………… programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.

A) Zombie

B) Worm

**C) Trojan Horses**

D) Logic Bomb

9. State whether true of false.

i) A worm mails a copy of itself to other systems.

ii) A worm executes a copy of itself on another system.

A) True, False

B) False, True

**C) True, True**

D) False, False

10. A ………….. is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs.

A) Worm

**B) Virus**

C) Zombie

D) Trap doors

**Answers:**

|  |  |
| --- | --- |
| **1.**       **B) Integrity**  **2.**       **A) Confidentiality**  **3.**       **C) i, ii, iii and v only**  **4.**       **D) Worm**  **5.**       **A) Trap doors** | **6.**       **C) Logic Bomb**  **7.**       **A) Trojan Horse**  **8.**       **C) Trojan Horses**  **9.**       **C) True, True**  **10.**   **B) Virus** |

[**Which of the following does NOT use a 'Cryptographical Technique' to protect data?**](http://www-students.doc.ic.ac.uk/~bk2/test.html#a2)  
a. the use of digital signatures  
b. data encryption  
**c. the use of stored encrypted password files**d. using asymmetric keys at 'sender' and 'receiver' nodes

]

[**What is the main purpose of access control?**](http://www-students.doc.ic.ac.uk/~bk2/test.html#a14)a. to authorise full access to authorised users **b. to limit the actions or operations that a legitimate user can perform**  
c. to stop unauthorised users accessing resourcesd. to protect computers from viral infections

SHA-l has a message digest of

1. **160 bits**
2. 512 bits
3. 628 bits
4. 820 bits

Answer A

: Message authentication is a service beyond

1. Message Confidentiality
2. **Message Integrity**
3. Message Splashing
4. Message Sending

Answer B

 In Message Confidentiality, transmitted message must make sense to only intended

1. **Receiver**
2. Sender
3. Third Party
4. Translator

Answer A

A hash function guarantees integrity of a message. It guarantees that message has not be

1. Replaced
2. Over view
3. **Changed**
4. Left

Answer C

: To check integrity of a message, or document, receiver creates the

1. Tag
2. **Hash Tag**
3. Hyper Text
4. Finger Print

 A digital signature needs a

1. private-key system
2. shared-key system
3. public-key system
4. All of them

Answer C

Answer B

 One way to preserve integrity of a document is through use of a

1. Thumb Impression
2. **Finger Print**
3. Biometric
4. X-Rays

Answer B

 A session symmetric key between two parties is used

1. **only once**
2. twice
3. multiple times
4. depends on situation

Answer A

Encryption and decryption provide secrecy, or confidentiality, but not

1. Authentication
2. **Integrity**
3. Keys
4. Frames

MAC stands for

1. **message authentication code**
2. message authentication connection
3. message authentication control
4. message authentication cipher

Digest created by a hash function is normally called a

1. **modification detection code (MDC)**
2. message authentication connection
3. message authentication control
4. message authentication cipher

Answer A Message confidentiality is using

1. Cipher Text
2. Cipher
3. Symmetric-Key
4. **Asymmetric-Key**

A sender must not be able to deny sending a message that he or she, in fact, did send, is known as

1. **Message Nonrepudiation**
2. Message Integrity
3. Message Confidentiality
4. Message Sending

Answer A

To preserve integrity of a document, both document and fingerprint are

1. Important
2. System
3. **Needed**
4. Not needed

Answer C

 When data must arrive at receiver exactly as they were sent, its called

1. Message Confidentiality
2. **Message Integrity**
3. Message Splashing
4. Message Sending

Message digest needs to be

1. public
2. private
3. **kept secret**
4. None

Answer C

In Message Integrity, message digest needs to be kept

1. **Secret**
2. Low
3. High
4. Down

Answer A

 In Message Integrity, SHA-l hash algorithms create an N-bit message digest out of a message of

1. **512 Bit Blocks**
2. 1001 Bit Blocks
3. 1510 Bit Blocks
4. 2020 Bit Blocks

Answer A

Message confidentiality or privacy means that sender and receiver expect

1. Integrity
2. **Confidentiality**
3. Authentication
4. Nonrepudiation

Answer B

AOne commonly used public-key cryptography method is the \_\_\_\_\_\_ algorithm.

* A)            RSS
* B)            RAS
* C)            RSA
* D)            RAA

The Vigenère cipher is an example of:

(A) a Cæsar cipher. (B) a monoalphabetic cipher. (C) a polyalphabetic cipher. (D) None of A,B,C.

\_\_\_\_\_\_ algorithm transforms ciphertext to plaintext.

* A)            encryption
* B)            decryption
* C)            either (a) or (b)
* D)            neither (a) nor (b)

The \_\_\_\_\_\_\_\_ is the message after transformation.

* A)            ciphertext
* B)            plaintext
* C)            secret-text
* D)            none of the above

A \_\_\_\_\_\_\_\_ cipher replaces one character with another character.

* A)            substitution
* B)            transposition
* C)            either (a) or (b)
* D)            neither (a) nor (b)

The \_\_\_\_\_\_\_\_ cipher reorders the plaintext characters to create a ciphertext.

* A)            substitution
* B)            transposition
* C)            either (a) or (b)
* D)            neither (a) nor (b)

The \_\_\_\_\_\_\_\_\_ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.

* A)             man-in-the-middle
* B)             ciphertext attack
* C)             plaintext attack
* D)             none of the above

In an asymmetric-key cipher, the receiver uses the \_\_\_\_\_\_ key.

* A)             private
* B)             public
* C)             either a or b
* D)             neither (a) nor (b)

DES uses a key generator to generate sixteen \_\_\_\_\_\_\_ round keys.

* A)             32-bit
* B)             48-bit
* C)             54-bit
* D)             42-bit

ECB and CBC are \_\_\_\_\_\_\_\_ ciphers.

* A)             block
* B)             stream
* C)             field
* D)             none of the above

In a(n) \_\_\_\_\_\_\_\_ cipher, the same key is used by both the sender and receiver.

* A)             symmetric-key
* B)             asymmetric-key
* C)             either (a) or (b)
* D)             neither (a) nor (b)

\_\_\_\_\_\_\_\_\_ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.

* A)             Substitution
* B)             Transposition
* C)             either (a) or (b)
* D)             neither (a) nor (b)

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  
View Answer

Answer:b

3. Which one of the following algorithm is not used in asymmetric-key cryptography?  
a) RSA algorithm  
b) diffie-hellman algorithm  
c) electronic code book algorithm  
d) none of the mentioned  
View Answer

Answer:c  
Explanation:None.

6. Cryptanalysis is used  
a) to find some insecurity in a cryptographic scheme  
b) to increase the speed  
c) to encrypt the data  
d) none of the mentioned  
View Answer

Answer:a  
Explanation:None.

7. Which one of the following is a cryptographic protocol used to secure HTTP connection?  
a) stream control transmission protocol (SCTP)  
b) transport layer security (TSL)  
c) explicit congestion notification (ECN)  
d) resource reservation protocol  
View Answer

Answer:b  
Explanation:None.

10. Cryptographic hash function takes an arbitrary block of data and returns  
a) fixed size bit string  
b) variable size bit string  
c) both (a) and (b)  
d) none of the mentioned  
View Answer

Answer:a  
Explanation:None.

Shift cipher is sometimes referred to as the

1. Caesar cipher
2. Shift cipher
3. cipher
4. cipher text

Answer A

Heart of Data Encryption Standard (DES), is the

1. Cipher
2. Rounds
3. Encryption
4. **DES function**

In Asymmetric-Key Cryptography, two keys, e and d, have a special relationship to

1. Others
2. Data
3. Keys
4. **Each other**

Answer D

 Substitutional cipers are

1. Monoalphabatic
2. Sami alphabetic
3. polyalphabetic
4. **both a and c**

Answer D

2) What is not a role of encryption ?  
a) It is used to protect data from unauthorized access during transmission  
b) It is used to ensure user authentication  
c) It is used to ensure data integrity  
d) It is used to ensure data corruption doesn’t happens  
View Answer

Answer: d

3) What is cipher-block chaining ?  
a) Data is logically ‘ANDed’ with previous block  
b) Data is logically ‘ORed’ with previous block  
c) Data is logically ‘XORed’ with previous block  
d) none of the mentioned  
View Answer

Answer: c

) What is not an encryption standard ?  
a) AES  
b) TES  
c) Triple DES  
d) DES  
View Answer

Answer: b  
Explanation: None.

6) What is a Hash Function ?  
a) It creates a small flexible block of data  
b) It creates a small,fixed block of data  
c) It creates a encrypted block of data  
d) none of the mentioned  
View Answer

Answer: b  
Explanation: None.

9) Which two of the following are authentication algorithms ?  
a) MAC  
b) AES  
c) DES  
d) Digital-signature  
View Answer

Answer: a & c  
Explanation: None.

10) What is role of Key Distribution Center ?  
a) It is used to distribute keys to everyone in world  
b) It intended to reduce the risks inherent in exchanging keys  
c) a and b both  
d) none of the mentioned  
View Answer

Answer: b  
Explanation: None.

Answer D

https://www.scribd.com/doc/229495035/Network-Security-Cryptography-MCQ-S  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRjIAnTG>  
  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRjCkMW6>  
  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRfBg2QR>  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRf6OJKY>  
  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRepYiSq>  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LReYnIQ1>  
Read more: <http://www.pinoybix.org/2014/04/cryptography-mcqs.html#ixzz4LRduqK38>

Answer A

Answer B