**CNS**

**(UNIT-1 & Half Of UNIT-2)**

1. Symmetric encrption alone is suitable for data encryption
   1. True
   2. False

ANSWER : B

1. A network security model comprises of
   1. Security related transformation
   2. Information Channel

C) Both A and B

D) Only B

ANSWER : C

1. Some of the network standadising organisations are
   1. NIST ,ISOC,IETF,IAB
   2. NIST,RFC
   3. ISOC,SP
   4. Both B and C

ANSWER : A

1. \_\_\_\_\_\_\_\_\_\_\_\_\_ is a U.S. federal agency that deals with measurement science, standards, and technology
   1. ISOC
   2. NIST
   3. IETF
   4. IAB

ANSWER : B

1. Conventional encryption, secret-key, or single-key encryption are the different names of
   1. Symmentric encryption
   2. Asymmentric encryption

C) Public key encryption

D) Both B and C

ANSWER : A

1. Along with plain text,encryption and decryption algorithm,cipher text ,\_\_\_\_\_\_ is also a ingredient of symmentric encryption
   1. Secret key
   2. Channel
   3. Firewall
   4. trusted third party

ANSWER : A

1. Cipher text obtained by a symmetric encryption algorithm is a function of input data and
   1. decryption algorithm
   2. key
   3. protocol
   4. both B and C

ANSWER : B

1. The security of symmetric encryption depends on
   1. the secrecy of the key
   2. secrecy of the algorithm
   3. Size of the input data
   4. All of these

ANSWER : A

1. Symmetric encryption algorithm performs
   1. Various substitutions and transformations
   2. Mathematical functions
   3. Sigmoid functions
   4. None of these

ANSWER : A

1. In symmetric encryption when different keys are used on same data, the resulting cipher text is same
   1. True
   2. False

ANSWER : B

1. With the success of symmetric encryption lying in not maintaining the secrecy of encryption algorithm has led to
   1. manufacturers develop low-cost chip implementations of data encryption algorithms
   2. feasible for widespread use
   3. Niether A nor B
   4. Both A and B

ANSWER : D

1. Cryptographic systems are classified as \_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_ based on the way the plaintext is processed
   1. Symmetric and Assymetric
   2. Assymetric and Substitution
   3. Stream cipher and Block Cipher
   4. Substitution cipher and Transposition cipher

ANSWER : C

1. A Cryptographic system where both sender and receiver use the same key is called
   1. Symmetric encryption.
   2. secret-key encryption.
   3. conventional encryption
   4. All of the above

ANSWER : D

1. The process of attempting to discover the plaintext or key is known
   1. Symmetric encryption.
   2. cryptanalysis.
   3. Intrusion
   4. All of the above

ANSWER : B

1. In a cryptanalysis ,if the type of attack is Ciphertext only then information know to cryptanalyst are
   1. Encryption algorithm and Ciphertext to be decoded
   2. Encryption algorithm and key
   3. Ciphertext to be decoded and key
   4. All of the above

ANSWER : A

1. An encryption scheme is computationally secure if the ciphertext generated by the scheme meets the following criteria
   1. The cost of breaking the cipher exceeds the value of the encrypted information

B)The time required to break the cipher exceeds the useful lifetime of the information

C) Both A and B

D) Only A

ANSWER: C

1. With the increase of \_\_\_\_\_\_\_ size and \_\_\_\_ size security of symmetric encryption is enhanced but with reduced encryption/decryption speed.
   1. Round function and Block
2. B)Key and Subkey generation algorithm
3. C)Block and key
4. D)rounds and Block

ANSWER: A

1. It is necessary to analyze the algorithm for cryptanalytic vulnerabilities with an intention of

A)feasibility for widespread use

B) Easy analysis of algorithm

C)develop a higher level of assurance as to its strength

D) All of the above

ANSWER: C

1. AES is a symmetric block cipher which supports for key lengths

A)128, 192, and 256

B) 64,128,256

C) 256,512,64

D) 192,196,256

ANSWER: A

1. AES is a symmetric block cipher which supports a block length of

A)64 bits

B)128 bits

C)56 bits

D)256 bits

ANSWER: A

1. AES uses Feistel structure for its process
   1. True
   2. False

ANSWER : B

1. Four different stages in the rounds of AES are

A) Substitute bytes, Shift rows, Add round key, Mix columns

B)Modulo 2 addition ,Shift column,Matrix multiplication,Substitute bytes

C)Mix Row,Add column,Shif column,Substitute bytes

D)XOR ,Modulo 2 addition ,Matrix multiplication

ANSWER: A

1. In AES the key that is provided as input is expanded into an array of \_\_\_\_\_\_\_\_\_\_\_\_ 32-bit words

A)64

B)128

C)44

D)256

ANSWER: C

1. \_\_\_\_\_\_\_ stage of AES makes use of the key

A)Mix row

B)Shift column

C) Add round key

D) Add function key

ANSWER: C

1. In decryption of AES algorithm ,the reverse of Add round key is performed using \_\_\_\_ function

A)AND

B)OR

C) XOR

D) both A and B

ANSWER: C

1. To break the plaintext into b-bit blocks how many modes of operation have been defined by NIST.
   1. 2
   2. 3
   3. 5
   4. 1

ANSWER: C

1. Following are the modes of operations that have been defined by NIST
   1. ECB
   2. CBC
   3. CFB
   4. All the above

ANSWER: D

1. Codebook is used in which mode
   1. ECB
   2. CBC
   3. CFB
   4. All the above

ANSWER: A

1. A mode which is used to convert any block cipher into a stream cipher is called
   1. cipher feedback mode
   2. Counter mode
   3. Cipher Block Chaining Mode
   4. electronic codebook mode

ANSWER: A

1. \_\_\_\_\_\_\_\_Mode is used in the applications of ATM (asynchronous transfer mode) network security and IPSec (IP security).
   1. cipher feedback mode
   2. Counter mode
   3. Cipher Block Chaining Mode
   4. electronic codebook mode

ANSWER: B

1. Public-key encryption is useful in
   1. Message Authentication only
   2. Key distribution only
   3. Both Message Authentication and Key Distribution.
   4. None Of the above

ANSWER: C

1. Public-key encryption, first publicly proposed by whom?
   1. Rivest
   2. Shamir
   3. Diffie and Hellman
   4. All the above

ANSWER: C

1. Public-key algorithms are based on\_\_\_\_\_\_\_\_\_\_\_\_\_
   1. Mathematical functions
   2. Operations on Bit patterns
   3. Multiplication
   4. None of the above

ANSWER: A

1. public-key cryptography is\_\_\_\_\_\_\_ , involving the use of\_\_\_\_\_\_\_\_separate keys.
   1. Asymmetric, Two
   2. Symmetric, One

ANSWER: A

1. Choose the Ingredients of Public key encryption Scheme
   1. Plaintext
   2. Ciphertext
   3. Public Key
   4. All the Above

ANSWER: D

1. The \_\_\_\_\_\_\_\_\_ performs various transformations on the plaintext is called
   1. Encryption Algorithm
   2. Decryption Algorithm
   3. Secure Hash Algorithm
   4. None of the Above

ANSWER: A

1. The \_\_\_\_\_\_\_\_\_\_ accepts the ciphertext and the matching key and produces the original plaintext.
   1. Encryption Algorithm
   2. Decryption Algorithm
   3. Secure Hash Algorithm
   4. None of the Above

ANSWER: B

1. Following are the applications of Public key Cryptosystem
   1. Encryption/Decryption
   2. Digital Signature
   3. Key Exchange
   4. All the Above

ANSWER: D

1. RSA algorithm can be used for the following applications
   1. Encryption/Decryption
   2. Digital Signature
   3. Key Exchange
   4. All the Above

ANSWER: D

1. Diffie-Hellman key exchange algorithm can be used for the following applications
   1. Encryption/Decryption
   2. Digital Signature
   3. Key Exchange
   4. All the Above

ANSWER: C

1. DSS algorithm can be used for the following applications
   1. Encryption/Decryption
   2. Digital Signature
   3. Key Exchange
   4. All the Above

ANSWER: B

1. It is computationally infeasible for an opponent, to determine the \_\_\_\_\_\_\_\_\_, by knowing the public key.
   1. Plaintext
   2. Ciphertext
   3. Secret Key
   4. Private Key

ANSWER: D

1. The two keys used for public-key encryption are referred to as the\_\_\_\_\_\_\_\_\_\_ and the\_\_\_\_\_\_\_\_\_\_\_\_.
   1. Public key,Private key
   2. Secret Key, Secret Key
   3. Hash, MAC
   4. NONE OF THE ABOVE

ANSWER: A

1. The sender encrypts a message with the recipient’s public key is known as
   1. Encryption
   2. Digital Signature
   3. Key Exchange
   4. All The Above

ANSWER: A

1. The sender “signs” a message with its private key is Known as
   1. Encryption
   2. Digital Signature
   3. Key Exchange
   4. All The Above

ANSWER: B

1. Both the sides of user cooperate to exchange a session key is known as
   1. Encryption
   2. Digital Signature
   3. Key Exchange
   4. All The Above

ANSWER: C

1. It is computationally easy for a any user to generate a pair of \_\_\_\_\_\_\_\_
   1. Keys
   2. Plaintext
   3. Ciphertext
   4. hashcode

ANSWER: A

1. The scrambled message produced depends on the plaintext and the key is called\_\_\_\_\_\_\_\_\_\_\_
   1. Plaintext
   2. Hash
   3. MAC
   4. Ciphertext

ANSWER: D

1. According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
   1. Confidentiality
   2. Integrity
   3. Authenticity
   4. Availability

ANSWER: C

1. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is “this” referred to here?
   1. Confidentiality
   2. Non-repudiation
   3. CIA Triad
   4. Authenticity

ANSWER: C

1. CIA triad is also known as \_\_\_\_\_\_\_\_
   1. NIC (Non-repudiation, Integrity, Confidentiality)
   2. AIC (Availability, Integrity, Confidentiality)
   3. AIN (Availability, Integrity, Non-repudiation)
   4. AIC (Authenticity, Integrity, Confidentiality)

ANSWER: D

1. When you use the word \_\_\_\_\_ it means you are protecting your data from getting disclosed.
   1. Confidentiality
   2. Integrity
   3. Authentication
   4. Availability

ANSWER: A

1. \_\_\_\_\_\_ means the protection of data from modification by unknown users.
   1. Confidentiality
   2. Integrity
   3. Authentication
   4. Non-repudiation

ANSWER: B

1. When integrity is lacking in a security system, \_\_\_\_\_\_\_\_\_ occurs.
   1. Database hacking
   2. Data deletion
   3. Data tampering
   4. Data leakage

ANSWER: C

1. \_\_\_\_\_\_\_ of information means, only authorised users are capable of accessing the information.
   1. Confidentiality
   2. Integrity
   3. Non-repudiation
   4. Availability

ANSWER: D

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

ANSWER: C

1. This helps in identifying the origin of information and authentic user. This referred to here as \_\_\_\_\_\_\_\_\_\_
   1. Confidentiality
   2. Integrity
   3. Authenticity
   4. Availability

ANSWER: C

1. Data \_\_\_\_\_\_\_\_\_\_\_ is used to ensure confidentiality.
   1. Encryption
   2. Locking
   3. Deleting
   4. Backup

ANSWER: A

Which of these is not a proper method of maintaining confidentiality?

* 1. Biometric verification
  2. ID and password based verification
  3. 2-factor authentication
  4. switching off the phone

ANSWER: D

1. Data integrity gets compromised when \_\_\_\_\_ and \_\_\_\_\_ are taken control off.
   1. Access control, file deletion
   2. Network, file permission
   3. Access control, file permission
   4. Network, system

ANSWER: C

1. \_\_\_\_\_\_ is the latest technology that faces an extra challenge because of CIA paradigm.
   1. Big data
   2. Database systems
   3. Cloud storages
   4. Smart dust

ANSWER: A

1. One common way to maintain data availability is \_\_\_\_\_\_\_\_\_\_
   1. Data clustering
   2. Data backup
   3. Data recovery
   4. Data Altering

ANSWER: B

1. \_\_\_\_\_\_\_\_\_\_\_\_\_ is a code injecting method used for attacking the database of a system / website.
   1. HTML injection
   2. SQL Injection
   3. Malicious code injection
   4. XML Injection

ANSWER: B

1. Which of them is not a wireless attack?
   1. Eavesdropping
   2. MAC Spoofing
   3. Wireless Hijacking
   4. Phishing

ANSWER: D

1. An attempt to harm, damage or cause threat to a system or network is broadly termed as \_\_\_\_\_\_
   1. Cyber-crime
   2. Cyber Attack
   3. System hijacking
   4. Digital crime

ANSWER: B

1. \_\_\_\_\_\_\_\_\_ are the special type of programs used for recording and tracking user’s keystroke.
   1. Keylogger
   2. Trojans
   3. Virus
   4. Worms

ANSWER: A

1. \_\_\_\_\_\_\_ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
   1. Network Security
   2. Database Security
   3. Information Security
   4. Physical Security

ANSWER: C

1. From the options below, which of them is not a threat to information security?
   1. Disaster
   2. Eavesdropping
   3. Information leakage
   4. Unchanged default password

ANSWER: D

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

ANSWER: A

1. \_\_\_\_\_ platforms are used for safety and protection of information in the cloud.
   1. Cloud workload protection platforms
   2. Cloud security protocols
   3. AWS
   4. One Drive

ANSWER: A

1. Which of the following information security technology is used for avoiding browser-based hacking?
   1. Anti-malware in browsers
   2. Remote browser access
   3. Adware remover in browsers
   4. Incognito mode in a browser

ANSWER: B

1. \_\_\_\_\_\_\_ technology is used for analyzing and monitoring traffic in network and information flow.
   1. Cloud access security brokers (CASBs)
   2. Managed detection and response (MDR)
   3. Network Security Firewall
   4. Network traffic analysis (NTA)

ANSWER: D

1. The full form of EDR is \_\_\_\_\_\_\_
   1. Endpoint Detection and recovery
   2. Early detection and response
   3. Endpoint Detection and response
   4. Endless Detection and Recovery

ANSWER: C

1. Compromising confidential information comes under \_\_\_\_\_\_\_\_\_
   1. Bug
   2. Threat
   3. Vulnerability
   4. Attack

ANSWER: B

1. Lack of access control policy is a \_\_\_\_\_\_\_\_\_\_\_\_\_
   1. Bug
   2. Threat
   3. Vulnerability
   4. Attack

ANSWER: C

1. Possible threat to any information cannot be \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   1. reduced
   2. transferred
   3. protected
   4. ignored

ANSWER: D

1. The key size of DES is
   1. 56 bits
   2. 64 bits
   3. 128 bits
   4. 168 bits

ANSWER: A

1. DES encrypts block of ...........bits
   1. 56 bits
   2. 64 bits
   3. 128 bits
   4. 168 bits

ANSWER: B

1. There are ......rounds in DES
   1. 8
   2. 10
   3. 14
   4. 16

ANSWER: D

1. DES stands for.........
   1. Digital Encryption Standard
   2. Decryption Encryption Standard
   3. Data Encryption Standard
   4. Data Enable Standard

ANSWER: C

1. During expansion permutation Right/Left Plain Text is Expanded from 32 to......bits
   1. 48 bits
   2. 64 bits
   3. 128 bits
   4. 56 bits

Answer: A

1. The heart of Data Encryption Standard (DES), is the
   1. Cipher
   2. Rounds
   3. Encryption
   4. DES function

ANSWER: D

1. Total no of S-boxes in DES is......
   1. 16
   2. 8
   3. 32
   4. 64

ANSWER: B

1. S-Box is referred as
   1. Standard Box
   2. Secquece Box
   3. Substitution Box
   4. Save Boxe

ANSWER: C

1. Tripple DES is DES......times
   1. 1
   2. 2
   3. 4
   4. 3

ANSWER: D

1. The 3 Key Tripple DES Decryption is as P=Dk1(Dk2(Dk3(C)))
   1. True
   2. False

ANSWER: A

1. The 3 Key Tripple DES Encryption is as C=Dk1(Dk2(Dk3(P)))
   1. True
   2. False

ANSWER: B

1. The 3 Key Tripple DES Decryption is as P=Ek1(Ek2(Ek3(C)))
   1. True
   2. False

ANSWER: B

1. The 3 Key Tripple DES Encryption is as C=Ek1(Dk2(Ek1(P)))
   1. True
   2. False

ANSWER: A

1. The 2 Key Tripple DES Decryption is as P=Dk1(Ek2(Dk1(C)))
   1. True
   2. False

ANSWER: A

1. FIPS stands for.......
   1. Federal Information Processing Standard
   2. First Information Processing Standard
   3. Fabric Information Processing Standard
   4. Further Information Processing Standard

ANSWER: A

1. DES follows a Feistel Sructure
   1. False
   2. True

ANSWER: B

1. DES follows
   1. Hash Algorithm
   2. Caesars Cipher
   3. Feistel Cipher Structure
   4. SP Networks

ANSWER: C

1. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
   1. True
   2. False

ANSWER: B

1. In the DES algorithm the round key is \_\_\_\_\_\_\_\_\_\_ bit and the Round Input is \_\_\_\_\_\_\_\_\_\_\_\_bits.
   1. 48, 32
   2. 64,32
   3. 56, 24
   4. 32, 32

ANSWER: A

1. The Initial Permutation table/matrix is of size
   1. 16×8
   2. 12×8
   3. 8×8
   4. 4×8

ANSWER: C

1. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
   1. True
   2. False

ANSWER: B

1. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 8th bit.
   1. True
   2. False

ANSWER: A

1. Data Encryption Standard (DES), was designed by
   1. Intel
   2. IBM
   3. HP
   4. Sony

ANSWER: B

1. Encryption standard that is selected by the US government to replace DES.
   1. AES
   2. BES
   3. CES
   4. DES

ANSWER: A

1. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
   1. Authenticated
   2. Joined
   3. Submit
   4. Separate

Answer A

1. let the RSA modulus n by 77 . If the encryption key is 37 then the decryption key is
   1. 13
   2. 29
   3. 43
   4. 58

Answer A

1. In RSA Algorithm the security relies on the difficulty of factoring large composite numbers
   1. true
   2. false

Answer A

1. In a RSA cryptosystem, a participant A uses two prime numbers p = 13 and q = 17 to generate her public and private keys. If the public key of A is 35, then the private key of A is \_\_\_\_\_\_\_.
   1. 11
   2. 29
   3. 43
   4. 58

Answer A

1. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice’s secret key is 4 and Bob’s secret key is 6, what is the secret key they exchanged?
   1. 16
   2. 17
   3. 18
   4. 19

Answer A

1. Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is-
   1. 3
   2. 4
   3. 5
   4. 6

Answer B

1. Public key cryptosystem is used for the encryption of
   1. Messages
   2. Session key
   3. Session key & Messages
   4. None of the above

Answer B

1. In asymmetric key cryptography, the private key is kept by \_\_\_\_\_\_\_\_\_\_
   1. sender
   2. receiver
   3. sender and receiver
   4. all the connected devices to the network

Answer B

1. Which one of the following algorithm is not used in asymmetric-key cryptography?
   1. rsa algorithm
   2. diffie-hellman algorithm
   3. electronic code book algorithm
   4. dsa algorithm

Answer C

1. Using p = 3, q = 13, d = 7 and e = 3 in the RSA algorithm, what is the value of ciphertext for a plain text 5 ?
   1. 8
   2. 16
   3. 26
   4. 33

Answer A

1. If we use the prime numbers 29 and 61 to generate keys using the RSA algorithm, then a possible choice of the public key could be
   1. 11
   2. 29
   3. 43
   4. 58

Answer A

1. The ciphertext obtained for message M = 2 when using RSA to perform encryption with A = 17, B = 31 and public key E = 7 is
   1. 64
   2. 128
   3. 162
   4. 212

Answer B

1. Suppose A and B use the Diffie-Hellman key exchange protocol with a common prime P = 71 and the primitive root = 7.If user A has private key KA= 5 and user B has private key KB= 12, then

the shared secret key is

* 1. 32
  2. 30
  3. 50
  4. 52

Answer B

1. Suppose, you are using RSA algorithm based cryptosystem to securely share the number of marbles that you have currently with you, among your friends. The private key that you are using is (3,15). Your friends know the corresponding public key is (11,15). One of your friends wants to sharethe exact amount of marble content only to you. What are the maximal possible marbles that your friend can have so that he/she can secretly share that to you?
   1. 14
   2. 29
   3. 43
   4. 58

Answer A

1. 10 parties want to exchange messages securely using some public key encryption Like RSA. the number of distinct key values reuired will be
   1. 10
   2. 25
   3. 40
   4. 20

Answer D

1. on what factor does the security of RSA algorithm depend upon
   1. on the difficulty of breaking large integers into prime numbers
   2. on the difficulty of solving discrete logarithm problems
   3. size of the key
   4. all of these

Answer A

1. one of the weakness of Diffie Hellman Key exchange algorithm is
   1. easily broken using Brute force attack
   2. Easily susceptible to Man in the Middle attack
   3. the key is small
   4. none of these

Answer B

1. If anyone is able to solve the Discrete Logarithm Problem (DLP), then he can easily solve \_\_\_\_\_\_\_\_\_\_\_\_ problem.
   1. DHKE problem
   2. RSA Problem

Answer A

1. Alice and Bob agree to use the prime P=5 and the primitive root g=2. Alice chooses the secret key a=4 and Bob chooses the secret key b= 3. Then, using Diffie-Hellman Key Exchange Protocol, the common secret key share between Alice and Bob is \_\_\_\_\_\_\_\_.
   1. 1
   2. 3
   3. 4
   4. 2

Answer A

1. Alice publishes her RSA public key: modulus N=77 and exponent e=37. Bob wants to send Alice the message m=2. What ciphertext does bob send to Alice?
   1. 51 (mod N)
   2. 15 (mod N)
   3. 55 (mod N)
   4. 52 (mod N)

Answer A

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ key exchange protocol based on discrete logarithm problem enables two parties to establish a common secret session key over unsecure communication channel.
   1. Micali-Schnorr
   2. ElGamal-Shamir
   3. Diffie-Hellman
   4. Miller-Rabin

Answer C

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can endanger the security of the Diffie-Hellman key exchange protocol if two parties are not authenticated to each other?
   1. Man-in-the-middle attack
   2. Ciphertext attack
   3. Plaintext attack
   4. None of the above

Answer A

**CNS**

**( Half Of UNIT-2 & UNIT-3)**

1. A hash function guarantees integrity of a message. It guarantees that message has not be
   1. Replaced
   2. Over view
   3. Changed
   4. Violated
2. Digest created by a hash function is normally called a.
   1. Message digest code (MDC)
   2. Modify authentication connection
   3. Message authentication control
   4. Message authentication cipher
3. Message authentication is a service beyond.
   1. Message Confidentiality
   2. Message Integrity
   3. Message Splashing
   4. Message Sending
4. Symmetric encrption alone is suitable for data encryption.
   1. True
   2. False
5. In Authentication without encryption ------- is not provided.
   1. Authentication
   2. Confidentiality
   3. Integrity
   4. None of the mentioned
6. Following are the examples of Message authentication Code.
   1. HMAC
   2. CMAC
   3. SHA-1
   4. Both A and B
7. SHA-l has a message digest of.
   1. 160 bits
   2. 512 bits
   3. 628 bits
   4. 820 bits
8. Hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string.The string is called the .
   1. Message digest
   2. Hash Value
   3. Checksum
   4. All of the mentioned
9. Message confidentiality is using.
   1. Cipher Text
   2. Cipher
   3. Symmetric-Key
   4. Asymmetric-Key
10. MAC is generated as a function of .
    1. Key
    2. Message
    3. secret code shared by communicating parties
    4. None of these
11. MAC is generated as a function of .
    1. Key
    2. Message
    3. Both A and B
    4. None of these
12. On generation of MAC,the reciver receives.
    1. Message
    2. MAC
    3. Both A and B
    4. Ciphertext
13. MAC stands for.
    1. Message authentication code
    2. Message arbitrary connection
    3. Message authentication control
    4. Message authentication cipher
14. Message \_\_\_\_\_\_\_ means that the receiver is ensured that the message is coming from the intended sender, not an intruder.
    1. Confidentiality
    2. Integrity
    3. Authentication
    4. None of the mentioned
15. Symmetric encryption with only sender and receiver sharing the key can achieve authentication.
    1. TRUE
    2. FALSE
16. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_supports in achieving authentication.
    1. Error detection code
    2. Sequence Number
    3. Time Stamp
    4. All of the mentioned
17. According to DAVI 89 , the situations in which message authentication without confidentiality Is preferred are.
    1. Broadcast of messages
    2. Heavy load system where decrypting is not affordable
    3. Both A and B
    4. None of the mentioned.
18. Hash function produces a fixed-length output accepting variable length data.
    1. TRUE
    2. FALSE
19. SHA-512 algorithm takes as input a message with a maximum length of less than.
    1. 2 ^ 128
    2. 2 ^ 192
    3. 2 ^112
    4. 2 ^ 64
20. SHA-512 algorithm has \_\_\_\_\_\_\_\_\_rounds in its function.
    1. 10
    2. 16
    3. 82
    4. 80
21. Confidentiality can only be provided if we perform message encryption before the MAC generation.
    1. True
    2. False
22. The digital signature provides authentication to the
    1. Sender
    2. Message
    3. Sender & Message
    4. None of the mentioned
23. The hash function \_\_\_\_\_\_\_\_\_\_\_
    1. Is collision free?
    2. Has manageable collision
    3. Has high unmanageable level of collision
    4. None of the mentioned
24. An alternative to message authentication code is.
    1. HMAC
    2. CMAC
    3. One-way-Hash function
    4. None of the mentioned
25. Name the hash function that is important not only in message authentication but in digital signatures.
    1. Secure hash function
    2. DES
    3. AES
    4. All the mentioned
26. SHA-256,SHA-384 and SHA-512 are collectively called as
    1. SHA-1
    2. SHA-2
    3. SHA-3
    4. SHA-4
27. In HMAC iPad represents\_\_\_\_\_\_\_.
    1. 00110110
    2. 01011100
    3. 11110011
    4. All the mentioned
28. In HMAC OPad represents\_\_\_\_\_\_\_.
    1. 00110110
    2. 01011100
    3. 11110011
    4. All the mentioned
29. Extensions were added in which version of Kerberos?
    * 1. 1
      2. 2
      3. 3
      4. 4
30. The subject unique identifier of the X.509 certificates was added in which version?
    * 1. 1
      2. 2
      3. 3
      4. 4
31. Which of the following is not an element/field of the X.509 certificates?
    * 1. Issuer Name
      2. Serial Modifier
      3. Issuer unique Identifier
      4. Signature
32. Suppose that A has obtained a certificate from certification authority X1 and B has obtained certificate authority from CA X2. A can use a chain of certificates to obtain B’s public key. In notation of X.509, this chain is represented in the correct order as –
    * 1. X2 X1 X1 B
      2. X1 X1 X2 A
      3. X1 X2 X2 B
      4. X1 X2 X2 A
33. Certificates generated by X that are the certificates of other CAs are Reverse Certificates.
    * 1. True
      2. False
34. It is desirable to revoke a certificate before it expires because
    * 1. the user is no longer certified by this CA
      2. the CA’s certificate is assumed to be compromised
      3. the user’s private key is assumed to be compromised
      4. all of the mentioned
35. CRL stands for
    * 1. Cipher Reusable List
      2. Certificate Revocation Language
      3. Certificate Revocation List
      4. Certificate Resolution Language
36. Which of the following is not a part of an Extension?
    * 1. Extension Identifier
      2. Extension value
      3. Criticality Indicator
      4. All of the mentioned constitute the Extension
37. The criticality indicator indicates whether an extension can be safely ignored.
    * 1. True
      2. False
38. “Conveys any desired X.500 directory attribute values for the subject of this certificate.”

Which Extension among the following does this refer to?

* + 1. Subject alternative name
    2. Issuer Alternative name
    3. Subject directory attributes
    4. None of the mentioned

1. Public key encryption/decryption is not preferred because
   * 1. it is slow
     2. it is hardware/software intensive
     3. it has a high computational load
     4. all of the mentioned
2. Which one of the following is not a public key distribution means?
   * 1. Public-Key Certificates
     2. Hashing Certificates
     3. Publicly available directories
     4. Public-Key authority
3. Which of the following public key distribution systems is most secure?
   * 1. Public-Key Certificates
     2. Public announcements
     3. Publicly available directories
     4. Public-Key authority
4. Which systems use a timestamp?
   * + 1. Public-Key Certificates
       2. Public announcements
       3. Publicly available directories
       4. Public-Key authority

i) and ii)

iii) and iv)

i) and iv)

iv) only

1. For each \_\_\_\_\_\_\_ the Kerberos Key Distribution Centre (KDC) maintains a database of the realm’s principal and the principal’s associated “secret keys”.
   * 1. key
     2. realm
     3. document
     4. none of the mentioned
2. Point out the correct statement.
   * 1. MongoDB Enterprise provides support for Kerberos authentication of MongoDB clients to mongod and mongos
     2. Kerberos is an industry standard authentication protocol for large client/server systems
     3. Kerberos allows MongoDB and applications to take advantage of existing authentication infrastructure and processes
     4. All of the mentioned
3. For a client-server authentication, the client requests from the KDC a \_\_\_\_\_\_\_\_ for access to a specific asset.
   * 1. ticket
     2. local
     3. token
     4. user
4. To authenticate using Kerberos, you must add the Kerberos user principals to MongoDB to the \_\_\_\_\_\_\_\_\_ database.
   * 1. $internal
     2. $external
     3. $extern
     4. None of the mentioned
5. To specify a different value for <service>, use \_\_\_\_\_\_\_\_ during the start-up of mongod.
   * 1. servicepwd
     2. serviceName
     3. servicelogin
     4. none of the mentioned
6. Linux systems can store Kerberos authentication keys for a service principal in \_\_\_\_\_\_ files.
   * 1. Client
     2. Server
     3. key tab
     4. All of the mentioned
7. A \_\_\_\_\_\_\_\_\_ is a trusted third party that assigns a symmetric key to two parties.
   * 1. KDC
     2. CA
     3. KDD
     4. None of the options
8. A\_\_\_\_\_\_\_\_ creates a secret key only between a member and the centre.
   * 1. CA
     2. KDC
     3. KDD
     4. None of the options
9. The secret key between members need to be created as a \_\_\_\_\_\_\_ key when two members contact KDC.
   * 1. Public
     2. Session
     3. Complimentary
     4. None of the options
10. \_\_\_\_\_\_\_\_\_\_\_\_ is a popular session key creator protocol that requires an authentication server and a ticket granting server.
    * 1. KDC
      2. Kerberos
      3. CA
      4. None of the options
11. A\_\_\_\_\_\_\_\_\_\_\_ is a federal or state organization that binds a publick key to an entity and issues a certificate.
    * 1. KDC
      2. Kerberos
      3. CA
      4. None of the options
12. A\_\_\_\_\_\_\_\_\_\_\_ is a hierarchical system that answers queries about key certification.
    * 1. KDC
      2. Kerberos
      3. CA
      4. None of the options
13. The secret key between members needs to be created as a \_\_\_\_\_\_ key when two members contact KDC.
    * 1. public
      2. session
      3. complimentary
      4. none of the options
14. In \_\_\_\_\_\_ there is a single path from the fully trusted authority to any certificate.
    * 1. X509
      2. PGP
      3. KDC
      4. none of the options
15. The denotation of certificate issuing, between Certificate issuing authority and applicant,
    * 1. CA<<A>>
      2. CA>>A
      3. CA<A>
      4. A<<CA>>
16. A Kerberos environment consists of
    * 1. a Kerberos server
      2. a number of clients, all registered with server
      3. application servers, sharing keys with server
      4. All
17. The property of hash function is said to be deterministic, if for a given input returns as output -----------
    1. Same hash value
    2. Different hash value
    3. Unique hash value
    4. Not mentioned
18. The property of hash function is said to be UNIFORM, if all the input bits influence the output hash.
    1. True
    2. False
19. If a single bit of the input string is flipped then each bit of the hash value is flipped with a probability roughly equal to ----
    1. 0.2
    2. 0.5
    3. 1.0
    4. 0.75
20. HASH function converts a plaintext of arbitrary size to a fixed size output.
    1. True
    2. False
21. HASH function makes use of a key
    1. True
    2. False
22. Hash functions are also called as ---------------
    1. message digest
    2. compression function
    3. encryption fucntion
    4. none of the mentioned
23. HASH function converts a plaintext of arbitrary size to a fixed size output called as
    1. Digest
    2. Hash value
    3. Hash
    4. all of the mentioned
24. Authentication is protection against active attacks
    1. True
    2. False
25. when a document is genuine and comes from an alleged source its said to be
    1. Authentication
    2. Integrity
    3. Confidentiality
    4. All of the mentioned
26. Authentication of message is possible through
    1. Ciphertext
    2. Message Authentication Code
    3. Hash Code
    4. All of the mentioned
27. Which of the following accepts variable size message and generates an authenticator without the use of the key
    1. Ciphertext
    2. Message Authentication Code
    3. Hash Code
    4. All of the mentioned
28. The property for any hash code 'h', and its computational infeasibility to find x such that H(x)=h
    1. One Way Hash Function
    2. Weak collision Resistant
    3. Strong Collision Resistant
    4. All the mentioned
29. The property for any hash code 'h', and its computational infeasibility to find x such that y=x with H(y)=H(x)
    1. One Way Hash Function
    2. Weak collision Resistant
    3. Strong Collision Resistant
    4. All the mentioned
30. The property for any hash code 'h', and its computational infeasibility to find a pair (x, y) such that H(y)=H(x)
    1. One Way Hash Function
    2. Weak collision Resistant
    3. Strong Collision Resistant
    4. All the mentioned
31. SHA1 and SHA-512 have output of
    1. 128 bit and 512 bits
    2. 128 bit and 256 bits
    3. 256 bit and 512 bits
    4. none of the mentioned
32. SHA-512 processes input of size of \_\_\_\_\_\_\_\_\_\_bits with \_\_\_\_\_\_\_\_\_rounds and \_\_\_\_\_\_\_\_\_\_\_ Buffers.
    1. 1024 bits, 80 , 6
    2. 512 bits, 80, 8
    3. 1024 bits, 80, 8
    4. 512 bits, 79, 6
33. Cryptographic hash functions execute faster in software than block ciphers.
    1. Statement is correct
    2. Statement is incorrect
    3. Depends on the hash function
    4. Depends on the processor
34. What is the value of ipad in the HMAC structure?
    1. 00111110
    2. 00110010
    3. 10110110
    4. 01110110
35. What is the value of opad in the HMAC structure?
    1. 00111110
    2. 00110010
    3. 10110110
    4. 01011100
36. What is the full-form of CMAC?
    1. Code-based MAC
    2. Cipher-based MAC
    3. Construct-based MAC
    4. Collective-based MAC
37. Which cryptographic algorithm is used in CMAC?
    1. Triple DES and AES
    2. DES
    3. RC-4
    4. AES
38. In CMAC, which scenario is a different key K2 is used instead of K1?
    1. If the tag is larger than the key length
    2. If the tag is shorter than the key length
    3. In the last step of the algorithm
    4. If the plaintext/message is not an integer multiple of the cipher clock length
39. K2 is derived by left shifting L by 2 bits. What is L defined as?
    1. E(K , 0b)
    2. E(K , 10\*b)
    3. E(K , 1b)
    4. E(K , 10\*1b)
40. Another name for Message authentication codes is
    1. cryptographic codebreak
    2. cryptographic codesum
    3. cryptographic checksum
    4. cryptographic checkbreak
41. For a 150-bit message and a 10-bit MAC, how many values are the MAC value dependent on?
    1. 2140
    2. 2150
    3. 215
    4. 210
42. Confidentiality can only be provided if we perform message encryption before the MAC generation.
    1. True
    2. False
43. MACs are also called
    1. testword
    2. checkword
    3. testbits
    4. none of the mentioned
44. For a 100 bit key and a 32 bit tag, how many possible keys can be produced in the 3rd round?
    1. 24
    2. 232
    3. 216
    4. 264
45. MAC is a
    1. one-to-one mapping
    2. many-to-one mapping
    3. onto mapping
    4. none of the mentioned
46. For an n-bit tag and a k-bit key, the level of effort required for brute force attack on a MAC algorithm is
    1. 2k
    2. 2n
    3. min(2k,2n)
    4. 2k/2n
47. A\_\_\_\_\_\_\_\_function creates a message digest out of a message.
    1. encryption
    2. decryption
    3. hash
    4. none of the mentioned
48. A \_\_\_\_\_\_\_ message digest is used as an MDC.
    1. keyless
    2. keyed
    3. either (a) or (b)
    4. neither (a) nor (b)
49. A \_\_\_\_\_\_\_\_ signature is included in the document; a \_\_\_\_\_\_\_ signature is a separate entity.
    1. conventional; digital
    2. digital; digital
    3. either (a) or (b)
    4. neither (a) nor (b)
50. Digital signature provides \_\_\_\_\_\_\_\_.
    1. authentication
    2. nonrepudiation
    3. both (a) and (b)
    4. neither (a) nor (b)
51. Digital signature cannot provide \_\_\_\_\_\_\_\_ for the message.
    1. integrity
    2. confidentiality
    3. nonrepudiation
    4. authentication
52. The \_\_\_\_\_\_\_ criterion states that it must be extremely difficult or impossible to create the message if the message digest is given.
    1. one-wayness
    2. weak-collision-resistance
    3. strong-collision-resistance
    4. none of the mentioned
53. The \_\_\_\_\_\_\_\_ criterion ensures that a message cannot easily be forged.
    1. one-wayness
    2. weak-collision-resistance
    3. strong-collision-resistance
    4. none of the mentioned
54. The \_\_\_\_\_\_\_criterion ensures that we cannot find two messages that hash to the same digest.
    1. one-wayness
    2. weak-collision-resistance
    3. strong-collision-resistance
    4. none of the mentioned
55. What is the number of round computation steps in the SHA-256 algorithm?
    1. 80
    2. 76
    3. 64
    4. 70
56. In SHA-512, the message is divided into blocks of size \_\_\_ bits for the hash computation.
    1. 1024
    2. 512
    3. 256
    4. 1248
57. \_\_\_\_\_\_\_\_enables the feature of securing remote logon,client/server,e-mail,file transfer and web access.
    1. IPSec
    2. SSL
    3. PGP
    4. none of the above
58. Applications of IPsec
    1. Secure branch office connectivity over the Internet
    2. Secure remote access over the Internet
    3. Enhancing electronic commerce security
    4. All the above
59. When IPsec is implemented in a Firewall,it provides strong security that can be applied to all crossing the perimeter of
    1. Firewall
    2. Etherenet Switch
    3. Gateway
    4. HUB
60. The principal feature of IPsec that enables it to support varied applications is
    1. It can encrypt and/or authenticate all traffic at the application level
    2. It can encrypt and/or authenticate all traffic at the IP level
    3. Both A and B
    4. Security at physical layer
61. IPsec protocol operate in networking devices such as
    1. router
    2. firewall
    3. Devices that connect each LAN to the outside world
    4. All of the above
62. In an IP security scenario,the data leaving the network device with IPSec will have
    1. IP Header ,IPsec header ,Secure IP Payload
    2. Only IP Header
    3. Both A and B
    4. None of the above
63. IPsec can be transparent to end users which means no need to train users on security mechanisms
    1. TRUE
    2. FALSE
64. IPsec in a firewall is resistant to bypass
    1. if all traffic use IP and the firewall as only means of entrance
    2. Irrespective of any entry,it would resist bypass
    3. Only from know source
    4. All of the mentioned
65. IPsec can play a vital role in the routing architecture which can assure
    1. A router advertisement
    2. A neighbor advertisement
    3. Unforged routing update
    4. All of the mentioned
66. IPsec is below the \_\_\_\_\_\_\_\_\_\_ and so is transparent to applications.
    1. Network layer
    2. Application layer
    3. Transport layer
    4. Physical layer
67. \_\_\_\_\_\_\_\_\_\_ document of the IPsec document covers the general concepts, security requirements, definitions,and mechanisms defining IPsec technology.
    1. Architecture
    2. Authentication Header
    3. Encapsulating Security Payload
    4. Internet Key Exchange
68. Encapsulating Security Payload of the IPsec document provide
    1. encryption
    2. combined encryption/authentication
    3. authentication
    4. encryption and combined encryption/authentication
69. IPsec provides security services at the IP layer by enabling a system to select
    1. required security protocols
    2. determine the algorithm(s) to use for the service(s),
    3. put in place any cryptographic keys required to provide the requested services
    4. All of the mentioned
70. IPsec provides Limited traffic flow confidentiality also as a service.
    1. TRUE
    2. FALSE
71. \_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_ are the two protocols used in IPsec to provide security.
    1. Authentication Header and Internet Key Exchange
    2. Authentication Header and Encapsulating Security Payload
    3. Encapsulating Security Payload and Internet Key Exchange
    4. RSA and Elliptic Curve
72. IPSec defines two protocols: \_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_.
    1. AH; SSL
    2. PGP; ESP
    3. AH; ESP
    4. none of the above
73. Both AH and ESP protocols of IPsec operate in
    1. Only tunnel mode
    2. Only transport mode
    3. Both tunnel and transport modes
    4. None of the mentioned
74. ESP in transport mode encrypts
    1. IP payload
    2. IP header and IP payload
    3. IP Header
    4. IP payload and not IP header
75. AH in transport mode authenticates the IP payload and selected portions of the IP header.
    1. TRUE
    2. FALSE
76. ESP in transport mode does
    1. Encryption
    2. Authentication
    3. Partial encryption and complete Authentication
    4. Complete Encryption and optional authentication
77. \_\_\_\_\_\_\_\_\_\_\_ mode is used when one or both ends of a security association (SA) are a security gateway
    1. Transport mode
    2. Tunnel mode
    3. Both A and B
    4. None of the mentioned
78. With tunnel mode, of hosts on networks behind firewalls cannot engage in secure communications without implementing IPsec
    1. TRUE
    2. FALSE
79. ESP consists of an encapsulating header and trailer used to provide
    1. Decryption
    2. Encryption/authentication.
    3. Confidentiality
    4. Digital Signature
80. \_\_\_\_\_\_\_\_\_\_\_\_is a collection of documents describing the key management schemes for use with IPsec.
    1. Internet Key Exchange
    2. Encapsulating Security payload
    3. Authentication Header
    4. both Internet Key Exchange and Encapsulating Security payload
81. IPsec provides following security services at the IP layer.
    1. Access control
    2. Connectionless integrity
    3. Data origin authentication
    4. All the mentioned
82. Typically which mode of IPSEC is used for end-to-end communication between two hosts.
    1. Transport Mode
    2. Tunnel Mode
    3. Both A and B
    4. None of the mentioned
83. Which mode extends protection to the payload of an IP packet
    1. Transport Mode
    2. Tunnel Mode
    3. Both A and B
    4. None of the mentioned
84. Which mode provides protection to the entire IP packet
    1. Transport Mode
    2. Tunnel Mode
    3. Both A and B
    4. None of the mentioned
85. \_\_\_\_\_\_ provides authentication at the IP level.
    1. AH
    2. ESP
    3. PGP
    4. SSL
86. \_\_\_\_\_\_ provides either authentication or encryption, or both, for packets at the IP level.
    1. AH
    2. ESP
    3. PGP
    4. SSL
87. Authentication header Authenticates IP payload and selected portions of IP header and IPv6 extension headers at\_\_\_\_\_\_\_\_\_\_\_\_mode.
    1. Transport Mode SA
    2. Tunnel Mode SA
    3. Both A and B
    4. None of the mentioned
88. Encapsulating Security Payload with authentication Encrypts entire inner IP packet and Authenticates inner IP packet.
    1. Transport Mode SA
    2. Tunnel Mode SA
    3. Both A and B
    4. None of the mentioned
89. In the \_\_\_\_\_\_ mode, IPSec protects information delivered from the transport layer to the network layer.
    1. transport
    2. tunnel
    3. either (a) or (b)
    4. neither (a) nor (b)
90. IPSec in the \_\_\_\_\_\_ mode does not protect the IP header.
    1. transport
    2. tunnel
    3. either (a) or (b)
    4. neither (a) nor (b)
91. Pretty good privacy (PGP) security system uses
    1. Public key cryptosystem
    2. Private key cryptosystem
    3. Public & Private key cryptosystem
    4. None of the mentioned
92. Public key cryptosystem is used for the encryption of
    1. Messages
    2. Session key
    3. Session key & Messages
    4. None of the mentioned
93. PGP offers \_\_\_\_\_ block ciphers for message encryption.
    1. Triple-DES
    2. CAST
    3. IDEA
    4. All of the mentioned
94. What is the key size allowed in PGP?
    1. 1024-1056
    2. 1024-4056
    3. 1024-4096
    4. 1024-2048
95. One security protocol for the e-mail system is \_\_\_\_\_\_\_\_\_.
    1. IPSec
    2. SSL
    3. PGP
    4. none of the above
96. \_\_\_\_\_\_\_\_ provides privacy, integrity, and authentication in e-mail.
    1. IPSec
    2. SSL
    3. PGP
    4. none of the above
97. In \_\_\_\_\_\_\_, the cryptographic algorithms and secrets are sent with the message.
    1. IPSec
    2. SSL
    3. TLS
    4. PGP
98. \_\_\_\_\_\_ was invented by Phil Zimmerman.
    1. IPSec
    2. SSL
    3. PGP
    4. none of the above
99. In PGP, to exchange e-mail messages, a user needs a ring of \_\_\_\_\_\_\_ keys.
    1. secret
    2. public
    3. either Secret or Public
    4. both Secret and Public
100. Pretty good privacy program is used for
     1. Electronic mails
     2. File encryption
     3. Electronic mails & File encryption
     4. None of the mentioned
101. PGP system uses
     1. Private key system
     2. Public key system
     3. Private & Public key system
     4. None of the mentioned
102. What is the PGP stand for?
     1. Permuted Gap Permission
     2. Permuted Great Privacy
     3. Pretty Good Permission
     4. None of the mentioned
103. PGP makes use of which cryptographic algorithm?
     1. DES
     2. AES
     3. RSA
     4. Rabin
104. Pretty good privacy (PGP) security system uses
     1. Public key cryptosystem
     2. Private key cryptosystem
     3. Public & Private key cryptosystem
     4. None of the mentioned
105. In PGP,there is \_\_\_\_\_\_\_\_\_from the fully or partially trusted authorities to any subject
     1. Multiple paths
     2. Two paths
     3. Single path
     4. ALLthe mentioned
106. When sending digital signatures, PGP uses an efficient algorithm that generates \_\_\_\_\_\_\_\_\_
     1. CipherText
     2. PlainText
     3. MAC
     4. HASH
107. PGP Provides authentication through the use of \_\_\_\_\_\_\_\_\_
     1. Digital Signature
     2. Encryption Algorithm
     3. Zip Algorithm
     4. Radix-64 Encoding Scheme
108. PGP Provides Confidentiality through the use of \_\_\_\_\_\_\_\_\_
     1. Digital Signature
     2. Symmetric Block Encryption
     3. Zip Algorithm
     4. Radix-64 Encoding Scheme
109. PGP Provides Compression through the use of \_\_\_\_\_\_\_\_\_
     1. Digital Signature
     2. Symmetric Block Encryption
     3. Zip Algorithm
     4. Radix-64 Encoding Scheme
110. PGP Provides E-mail Compatability through the use of \_\_\_\_\_\_\_\_\_
     1. Digital Signature
     2. Symmetric Block Encryption
     3. Zip Algorithm
     4. Radix-64 Encoding Scheme
111. In PGP, message is encrypted using
     1. CAST-128
     2. DES
     3. AES
     4. MD5
112. PGP uses a variant of Diffie-Hellman that does provide encryption/decryption, known as
     1. BlowFish
     2. Diffie-Hellman
     3. ElGamal
     4. None of the mentioned
113. The use of Radix-64 in PGP Expand the Message By
     1. 50%
     2. 33%
     3. 30%
     4. 15%
114. PGP makes use of how many types of keys
     1. 2
     2. 3
     3. 4
     4. 1
115. PGP message has got how many components?
     1. 1
     2. 2
     3. 3
     4. NONE
116. Following are the Components of PGP message
     1. Message,Signature and Session Key
     2. Message
     3. Signature
     4. All the Mentioned Choices.
117. Signature Component of PGP Includes
     1. Timestamp,Message Digest and Leading Two Octets of message Digest
     2. Message Digest
     3. Timestamp
     4. Ciphertext
118. PGP makes use of following algorithms as a package for Public key encryption
     1. RSA, DSS adn Diffie-Hellman
     2. Diffie-Hellman
     3. RSA
     4. DSS
119. PGP makes use of following algorithms as a package for Symmetric key encryption
     1. CAST-128
     2. IDEA
     3. CAST-128, IDEA and 3DES
     4. None of the mentioned
120. PGP makes use of following algorithm for generating HASH CODE
     1. SHA-512
     2. SHA-256
     3. SHA-2
     4. SHA-1
121. PGP makes use of following types of keys
     1. session key , secret key , public and private key
     2. session key, public key , private key and passphrase based key
     3. public key and private key
     4. one time session key
122. IDEA uses\_\_\_\_\_\_keys
     1. 56 bit
     2. 128 bit
     3. 254 bit
     4. 512 bit
123. 3DES uses\_\_\_\_\_keys.
     1. 56 bit
     2. 128 bit
     3. 168 bit
     4. 512 bit
124. MIME transfer encoding's objective is to provide
     1. reliable delivery across the largest range of environments.
     2. enables fragmentation of a large message into a number of parts
     3. enables the construction of a message
     4. All of the mentioned
125. S/MIME is very similar to PGP. Both offer the ability to
     1. sign
     2. encrypt
     3. Both sign and encrypt
     4. None of the mentioned
126. S/MIME provides the following functions i) Enveloped data ii) Signed data iii) Clear-signed data iv) Signed and enveloped data
     1. i) ,ii) and iii)
     2. i) ,ii) iii) and iv)
     3. None
     4. Only i)
127. MIME transfer encoding's objective is to provide
     1. reliable delivery across the largest range of environments.
     2. enables fragmentation of a large message into a number of parts
     3. enables the construction of a message
     4. All of the mentioned
128. S/MIME is very similar to PGP. Both offer the ability to
     1. sign
     2. encrypt
     3. Both Sign and Encrypt
     4. None of the mentioned
129. S/MIME provides ----------- functions
     1. Enveloped data
     2. Clear-signed data
     3. Signed data
     4. All of the mentioned
130. MIME is intended to resolve some SMTP problems viz
     1. Deletion, addition, or reordering of carriage return and linefeed
     2. Truncating or wrapping lines longer than 76 characters
     3. Only Deletion
     4. Only Addition
131. S/MIME is not similar to
     1. TRUE
     2. FALSE
132. The header field Content-Description in MIME describes -----------------
     1. The text description when the object is not readable
     2. The transformation
     3. The identity of MIME entities
     4. Both Transformation and identity of MIME
133. Full Form of S/MIME
     1. Secured/ Multipurpose Internet Mail Extension
     2. Security/Multiple Intranet Mail Extended
     3. Secured/ Multipurpose Intranet Mail Extension
     4. None of the mentioned
134. S/MIME is used for\_\_\_\_\_\_ PGP is used for\_\_\_\_\_\_\_\_
     1. Commercial, Personnel
     2. Personnel, Commercial
     3. Commercial, Commercial
     4. Personnel, Personnel
135. In RFC5322 context, Messages as having an \_\_\_\_\_\_ and \_\_\_\_\_\_
     1. Data and Image
     2. Data and Data
     3. Envelope and Contents
     4. Information and Contents
136. According to RFC2046 specification , MIME has got\_\_\_\_\_types of contents and \_\_\_\_\_\_Subtypes.
     1. 3 , 5
     2. 5, 5
     3. 7, 15
     4. 1,1
137. In MIME, Digest comes under which Content type
     1. Type
     2. Video
     3. Audio
     4. Multipart
138. In MIME, jpeg and gif comes under which Content type
     1. Image
     2. Video
     3. Audio
     4. Multipart

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | A | B | B | B | D | A | D | D | D |
| C | C | A | C | A | D | C | A | A | D |
| B | C | A | C | A | B | A | B | C | B |
| B | C | A | D | C | D | A | C | D | B |
| A | C | B | D | A | B | B | C | A | B |
| B | B | C | C | B | C | A | D | A | A |
| B | A | B | B | D | A | A | D | D | A |
| B | C | C | C | D | B | D | B | A | D |
| A | C | A | B | D | A | B | C | C | A |
| A | C | B | A | B | C | A | A | A | D |
| A | B | D | A | A | A | D | C | A | D |
| D | A | B | C | C | D | A | D | B | B |
| B | A | D | A | A | B | A | B | A | B |
| A | A | C | B | D | C | C | C | D | C |
| B | C | C | C | C | C | A | D | A | B |
| C | D | A | C | B | C | C | A | A | A |
| C | D | B | B | C | A | C | B | A | C |
| D | B | B | A | A | A | C | C | D | A |
|  |  |  |  |  |  |  |  |  |  |

**CNS**

**(UNIT-4)**

1. The two most publicized threats to security is the. .......... and...........
   1. Intruder & Virus
   2. Firewall & Virus
   3. Firewall & Intruder
   4. Antivirus & Firewall

ANSWER: A

1. Intruder is also referred to as a........ Or.........
   1. Hacker or racker
   2. Hacker or cracker
   3. Cracker or racker
   4. Craker or backer

ANSWER: B

1. How many classes of Intrusions are mainly identified by intruders?
   1. 1
   2. 2
   3. 3
   4. 4

ANSWER: C

1. An individual who is not authorized to use the computer but penetrates a system’s access controls to exploit a legitimate user’s account is called as
   1. Clandestine user
   2. Misfeasor
   3. Virus
   4. Masquerade

ANSWER: D

1. A legitimate user who accesses data, programs, or resources for which such access is not authorized is called
   1. Clandestine user
   2. Misfeasor
   3. Virus
   4. Masquerade

ANSWER: B

1. An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection is called
   1. Clandestine user
   2. Misfeasor
   3. Virus
   4. Masquerade

ANSWER: A

1. The techniques and behaviour patterns of intruders are constantly
   1. Moving
   2. Increasing
   3. Shifting
   4. Decreasing

ANSWER: C

1. The CERTs stands for......
   1. Computer emergency response teams
   2. Computer emergency response times
   3. Computer emergency report times
   4. Computer emergency report teams

ANSWER: A

1. The password file can be protected in one of
   1. Three ways
   2. Four ways
   3. Two ways
   4. Five ways

ANSWER: C

1. How many no of approaches are there for intrusion detection?
   1. 1
   2. 3
   3. 4
   4. 2

ANSWER: D

1. The approach which involves defining thresholds, independent of user, for the frequency of occurrence of various events is called
   1. Profile based
   2. Threshold detection
   3. Anomaly detection
   4. Penetration identification

ANSWER: B

1. A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts is called
   1. Penetration identification
   2. Threshold detection
   3. Anomaly detection
   4. Profile based

ANSWER: D

1. Rules are developed to detect deviation from previous usage patterns is known as
   1. Penetration identification
   2. Threshold detection
   3. Anomaly detection
   4. Profile based

ANSWER: C

1. An expert system approach that searches for suspicious behaviour is called
   1. Penetration identification
   2. Threshold detection
   3. Anomaly detection
   4. Profile based

ANSWER: A

1. A fundamental tool for intrusion detection is
   1. Native audit records
   2. Detection-specific audit records
   3. Anomaly Record
   4. Audit Records

ANSWER: D

1. Honeypots are
   1. Virus
   2. Anti-virus
   3. Intrusion detection technology
   4. Intruder

ANSWER: C

1. A ...........model is used to establish transition probabilities among various states
   1. Multivariate
   2. Markov process
   3. Time series
   4. Operational

ANSWER: B

1. A ......... model is based on correlations between two or more variables.
   1. Multivariate
   2. Markov process
   3. Time series
   4. Operational

ANSWER: A

1. A ......... model focuses on time intervals, looking for sequences of events that happen too rapidly or too slowly
   1. Multivariate
   2. Markov process
   3. Time series
   4. Operational

ANSWER: C

1. A ..........model , based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records is
   1. Multivariate
   2. Markov process
   3. Time series
   4. Operational

ANSWER: D

1. A nonnegative integer that may be incremented but not decremented until it is reset by management action is Counter.
   1. True
   2. False

ANSWER: A

1. A nonnegative integer that may be incremented or decremented is Gauge
   1. True
   2. False

ANSWER: A

1. A nonnegative integer that may be incremented but not decremented until it is reset by management action is Gauge.
   1. True
   2. False

ANSWER: B

1. A nonnegative integer that may be incremented or decremented is Counter
   1. True
   2. False

ANSWER: B

1. Crypt(3) is based on which algorithm
   1. AES
   2. DES
   3. RSA
   4. DSS

ANSWER: B

1. Which of the following statements are true with respect to SALT
   1. It prevents duplicate password
   2. Increases the length of the password
   3. Ease to crack the password
   4. It prevents duplicate password and Increases the length of the password

ANSWER: D

1. System hacking involves password hacking as one of the major hacking methodologies.
   1. True
   2. False

ANSWER: A

1. There are \_\_\_\_\_\_\_\_ major types of passwords.
   * 1. 4
     2. 5
     3. 6
     4. 7

ANSWER: D

1. Basic technique involved in password selection strategy
   1. User Education
   2. Computer-generated passwords
   3. Reactive Password checking
   4. All the mentioned

AMSWER: D

1. Most promising approach to improved password security is
   1. User Education
   2. Computer-generated passwords
   3. Reactive Password checking
   4. Pro-active password checking

ANSWER: D

1. Markov Model is
   1. Tuple
   2. quadruple
   3. Matrix
   4. None of the mentioned

ANSWER: B

1. In \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attacks an attacker do not contact with authorizing party for stealing password.
   1. passive online
   2. active online
   3. offline
   4. non-electronic

ANSWER: A

1. Two possible problems with computer generated passwords are
   1. Time and Space
   2. Trust and Time
   3. None of the mentioned
   4. Date and Time

ANSWER: A

1. Trick with proactive password checker is
   1. User acceptability and strength
   2. Password selection
   3. User selection
   4. None of the mentioned

ANSWER: A

1. In Markov model tuple m stands for
   1. No of states in the model
   2. Matrix
   3. State space
   4. Order of the model

ANSWER: A

1. In Markov model tuple A stands for
   1. No of states in the model
   2. Matrix
   3. State space
   4. Order of the model

ANSWER: C

1. In Markov model tuple T stands for
   1. No of states in the model
   2. Matrix of transition probabilities
   3. State space
   4. Order of the model

ANSWER: B

1. In Markov model tuple k stands for
   1. No of states in the model
   2. Matrix of transition probabilities
   3. State space
   4. Order of the model

ANSWER: D

1. Malicious software that need a host program and cannot exist independently are called
   1. Independent malware
   2. parasitic
   3. logic bombs
   4. bots

ANSWER: B

1. Examples of parasitic malware are
   1. Viruses, logic bombs
   2. Worms and bot programs
   3. backdoors
   4. viruses, logic bombs and backdoors

ANSWER: D

1. logic bombs, backdoors, and bot programs are examples of malware that
   1. do not replicate
   2. replicate
   3. parasitic
   4. All the mentioned

ANSWER: A

1. backdoors used by Programmers legitimately for many years to debug and test programs is called

A) Trojan horse

B) Maintenance hook

C) malware

D) none of the mentioned

ANSWER: B

1. \_\_\_\_\_\_\_\_\_\_\_ is a malware code embedded in some legitimate program that is set to “explode” when certain conditions are met
   1. Trojan horse
   2. Logic bomb
   3. bot
   4. worm

ANSWER: B

1. Quietly deleting the user’s files is also the objective of the following malware apart from gaining access to the files of another user
   1. Trojan horse
   2. Logic bomb
   3. bot
   4. worm

ANSWER: A

1. Following are the examples of the multiple-threat malware
   1. multipartite
   2. blended attack
   3. Both A and B
   4. Only A

ANSWER : C

1. The different parts of virus are
   1. Infection mechanism, Trigger and Payload
   2. Trigger, dormant and propagation
   3. boot sector ,file infector, Macro virus
   4. None of the mentioned

ANSWER: A

1. \_\_\_\_\_\_\_\_\_\_\_\_ indicates the means by which a virus spreads, enabling it to replicate
   1. Trigger
   2. Payload
   3. Infection vector
   4. None of the above

ANSWER : C

1. In \_\_\_\_\_\_\_\_\_\_\_ phase virus is idle eventually be activated by some event, such as a date
   1. Dormant phase
   2. Propagation phase
   3. Triggering phase
   4. Execution phase:

ANSWER : A

1. In \_\_\_\_\_\_\_\_\_\_\_ phase the virus places a copy of itself into other programs or into certain system areas on the disk
   1. Dormant phase
   2. Propagation phase
   3. Triggering phase
   4. Execution phase:

ANSWER: B

1. In \_\_\_\_\_\_\_\_\_\_\_ phase the virus is activated to perform the function for which it

was intended

* 1. Dormant phase
  2. Propagation phase
  3. Triggering phase
  4. Execution phase:

ANSWER: C

1. In \_\_\_\_\_\_\_\_\_\_\_ phase the function of a virus is performed
   1. Dormant phase
   2. Propagation phase
   3. Triggering phase
   4. Execution phase

ANSWER: D

1. Following are the strategies for the classification of viruses
   1. target
   2. concealment strategy
   3. target and concealment strategy
   4. None of the mentioned

ANSWER: B

1. \_\_\_\_\_\_\_\_\_\_\_ virus infects files with macro code that is interpreted by an application.
   1. Boot sector infector
   2. File infector
   3. Macro virus
   4. Encrypted virus:

ANSWER: C

1. The virus that rewrites itself completely at each iteration, increasing the difficulty of detection
   1. Stealth virus
   2. Metamorphic virus
   3. Polymorphic virus
   4. Encrypted virus

ANSWER: B

1. Generic decryption and digital immune system are examples of
   1. Secure branch office connectivity over the Internet
   2. Secure remote access over the Internet
   3. Advanced Antivirus Techniques
   4. None of the mentioned

ANSWER: C

1. Applications of IPsec
   1. Secure branch office connectivity over the Internet
   2. Secure remote access over the Internet
   3. Enhancing electronic commerce security
   4. All the mentioned

ANSWER: D

1. Applications of IPsec
   1. Secure branch office connectivity over the Internet
   2. Secure remote access over the Internet
   3. Enhancing electronic commerce security
   4. All the mentioned

ANSWER: D

1. Applications of IPsec
   1. Secure branch office connectivity over the Internet
   2. Secure remote access over the Internet
   3. Enhancing electronic commerce security
   4. All the mentioned

ANSWER: D

1. Network layer firewall works as a \_\_\_\_\_\_\_\_\_\_
   * + 1. Frame filter
       2. Packet filter
       3. Content filter
       4. Virus filter

ANSWER: B

1. Network layer firewall has two sub-categories as \_\_\_\_\_\_\_\_\_
   * + 1. State full firewall and stateless firewall
       2. Bit oriented firewall and byte oriented firewall
       3. Frame firewall and packet firewall
       4. Network layer firewall and session layer firewall

ANSWER: A

1. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as \_\_\_\_\_\_\_\_\_\_
   * + 1. Chock point
       2. Meeting point
       3. Firewall point
       4. Secure point

ANSWER: A

1. Which of the following is / are the types of firewall?
   * + 1. Packet Filtering Firewall
       2. Dual Homed Gateway Firewall
       3. Screen Host Firewall
       4. Dual Host Firewall

ANSWER: A

1. A proxy firewall filters at \_\_\_\_\_\_\_\_\_
   * + 1. Physical layer
       2. Data link layer
       3. Network layer
       4. Application layer

ANSWER: D

1. A packet filter firewall filters at \_\_\_\_\_\_\_\_\_\_
   * + 1. Physical layer
       2. Data link layer
       3. Network layer or Transport layer
       4. Application layer

ANSWER: C

1. What is one advantage of setting up a DMZ with two firewalls?
   * + 1. You can control where traffic goes in three networks
       2. You can do stateful packet filtering
       3. You can do load balancing
       4. Improved network performance

ANSWER: C

1. What tells a firewall how to reassemble a data stream that has been divided into packets?
   * + 1. The source routing feature
       2. The number in the header’s identification field
       3. The destination IP address
       4. The header checksum field in the packet header

ANSWER: A

1. A stateful firewall maintains a \_\_\_\_\_\_\_\_\_\_\_ which is a list of active connections.
   * + 1. Routing table
       2. Bridging table
       3. State table
       4. Connection table

ANSWER: A

1. A firewall needs to be \_\_\_\_\_\_\_\_\_\_ so that it can grow proportionally with the network that it protects.
   * + 1. Robust
       2. Expansive
       3. Fast
       4. Scalable

ANSWER: B

1. A firewall is a \_\_\_\_\_\_security system:
   * + 1. Network
       2. File
       3. Program
       4. None of These

ANSWER: A

1. A firewall is a network security system \_\_\_\_\_\_based that controls incoming and outgoing network traffic based on a set of rules:
   * + 1. Hardware
       2. Software
       3. Both hardware or software
       4. None of These

ANSWER: C

1. Which among the following is correct:
   * + 1. A firewall is a system designed to prevent unauthorized access to or from a private network.
       2. Firewalls can be implemented in both hardware and software or a combination of both.
       3. Both
       4. None of the mentioned

ANSWER: C

1. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet especially \_\_\_\_:
   * + 1. Intranets
       2. Extranets
       3. Both
       4. None of The mentioned

ANSWER: A

1. Firewalls are used to protect:
   * + 1. Home Networks
       2. Corporate Networks
       3. Both
       4. None of The mentioned

ANSWER: C

1. If you have more than one computer connected in the home, it is important to protect every computer. You should have a \_\_\_\_firewall (such as a router) to protect your network:
   * + 1. Hardware
       2. Software
       3. HTML
       4. None of The mentioned

ANSWER: A

1. \_\_\_\_intercepts all messages entering and leaving the network. The \_\_\_\_\_effectively hides the true network addresses:
   * + 1. Circuit Level Gateway
       2. Proxy Server
       3. Packet Filter
       4. None of The mentioned

ANSWER: B

1. Firewalls are often categorized as:
   * + 1. Network Firewalls
       2. Host Based Firewalls
       3. Either Network firewalls or Host based firewalls
       4. None of The mentioned

ANSWER: C

1. Which among the following is correct:
   * + 1. Network firewalls are a software appliance running on general purpose hardware or hardware based firewall computer appliances that filter traffic between two or more networks.
       2. Host - based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine
       3. Both
       4. None of The mentioned

ANSWER: C

1. The first type of firewall was the packet filter which looks at:
   * + 1. network addresses
       2. Ports of the packet and determines if that packet should be allowed or blocked
       3. Both
       4. None of The mentioned

ANSWER: C

1. Application layer firewalls works on the application level of the \_\_\_\_stack (i.e. all browser traffic or all telnet or FTP traffic) and may intercept all packets travelling to or from an application:
   * + 1. TCP
       2. IP
       3. Both
       4. None of The mentioned

ANSWER: C

1. Which among the following is correct characteristics about proxy server:
   * + 1. A proxy server may act as a firewall by responding to input packets in the manner of an application while blocking other packets.
       2. A proxy server is a gateway from one network to another for a specific network application
       3. It performs its tasks or functions as a proxy on behalf of the network user;
       4. All OPTIONS

ANSWER: D