CNS Objective Questions With Answers
UNIT-1

1. Interception is ----------
   a) security service b**) security attack** c) security mechanism d) security strip
2. Interruption is attack on----------
   a) norepudiation b) **availability** c) authentication d) confidentiality
3. Fabrication is attack on----------
   a**)**nonrepudiation b) **availability** c) authentication d) confidentiality
4. Expansion of C2B is--------
   a) customer to branch b) branch to customer
   c**) customer to business** d) two way of branch and customer
5. Odd man out
   a) interruption b)**interception** c)modification d) fabrication
6. ---------- attack is capturing authorization privileges and used them later.
   a).modification b) masquerade c) **replay** d)denial of service
7. Cutting of communication line is an example of ----------
   a) **interruption** b) interception c)modification d) fabrication
8. which of the following integrity is not valid category of integrity
   a) connection integrity b) connectionless integrity
   c) field integrity d) **field less integrity**
9. Security service ---------- is requires that neither the sender nr the receiver of a message be able to deny the transmission.
   a**) nonrepudiation** b) availability c) authentication d) confidentiality
10. Vernam cipher is also called

a)rail fence b)**one time pad** c)book cipher d)running key cipher

11. DOS attacks are caused by

a)authentication b)alteration c)**fabrication** d)replay attacks

12. The process of writing the text as diagonals and reading it as a sequence of rows is known as

a**)rail fence** b)caesar cipher c)mono alphabetic d) vernam cipher

13. ----------is a technique that facilitates hiding of a message that is to be kept secret inside other messages

steganography

14. Science and art of developing cryptosystems is known as---------- **cryptography**

15.----------is the scrambled message or data that is generated as output by encryption algorithm **cipher text**

16. --------- attack take place when one entity pretends to different entity **masquerade**

17.----------ensures that only authorized parties are able to modify computer system data and transmitted information **integrity**

18. A process which is designed to detect, prevent or recover from an attack is known as ------ **Security mechanism**

19.----------means identifying origin of message correctly and it should ensures that identity is not false **authentication**

20. Any action that compromises the security of data which is owned by an organization is known as ----------**security attack**

UNIT II

1. DES stands for ----------
   (a) data entity standard (b) **data encryption standard** (c) data encryption software (d) digital encryption standard
2. DES is ----------
   (a) public key algorithm (b) **private key algorithm**
   (b) (c) key public algorithm (d) stream cipher

3. Simple DES(S-DES) contains---------- no. of bits for plain text

   (a) 10 bits (b) **8 bits** (c) 12 bots (d) 16 bits

4. AES requires ----------no.of bits for plain text

   (a) **128 bits** (b) 164 bits (c) 64 bits (d) 156 bits

5. The charcters in a word are arranged in random order it is called as -----

   (a**). permutation** (b) substitution (c) combination (d) expansion

6.Substitution – Permutation first introduced by ----------
   (a) Caesar (b) **shanon** (c) diffie (d) rivest

7. Number of rounds in DES ----------

   (a) 8 rounds (b**) 16 rounds** (c) 4 rounds (d) 32 rounds

8.Each S-box takes 6 bits input and produces ---- bits as output.

   (a) **4** (b) 8 (c)16 (d) 32

9. Number of S-boxes used in DES algorithm is --------

   (a) 4 (b) **8** (c)16 (d) 32

10.In ----------one bit of plain text is encrypted at a time

a)**stream cipher** b)block cipher c) both a & b d) none

11. In general private key encryption algorithms uses ----- no. of keys.**1**
12. Public key encryption algorithm uses ---- no. of keys .**2**
13. RSA algorithm was developed by---------**rivest Shamir adleman**
14. IDEA stands for---------**international data encryption algorithm**
15. CBC stands for ----------**cipher block chaining**
16. DES encrypts blocks of ---------- bits**64**
17. AES requires ---------- no of bits for plain text **128**
18. No of S- boxes used in Blowfish algorithm is ---------- 4
19. There are ----------rounds in Blowfish **16**
20. In ----------one block of plain text is encrypted at a time **block cipher**

UNIT III

1.Kerberos is ----------service designed for use in a distributed environment
a)integrity b) confidentiality c) **authentication** d) availability

2. -------- is a message digest algorithm
a) DES b)IDEA c) **MD5** d) RSA

3. When a hash function is used to provide message authentication, the hash function value is reffered to as ----
a) **message digest** b) message field c) message score d) message leap

4. X.509 scheme is -----certificate
a) Private key b) **public key** c) symmetric key d) none

5. MAC is also called-----
a)Cryptographic checksum b) fingerprint c) message digest d**) all the above**

6. Hash function can be applied to a block of ----
a) fixed size b) **variable size** c) 512 bytes d) 1024 bytes

7. SHA -512 uses -----registers
a) **8** b) 6 c) 4 d)5

8. SHA follows --- format to store values
a) littleenidian b) **big enidian** c) both a & b d) none

9.Number of steps in SHA-512-------

a) 60 b)70 c)**80** d) 40

10.Kerberos makes use of ------ algorithm

a) RSA b)**DES** c) Blowfish d) IDEA

11. SHA represents----------**secure hash algorithm**

12. Each block size of SHA -512 is ----------**128 bit**

13. SHA -512 algorithm outputs ----------bit message digest**512 bit**

14. TGS stands for----------**ticket granting server**

15. A ---------- can issue digital certificates**certificate authority**

16. The ----------standard defines the structure of a digital certificate**igital signature standard**

17. A full service Kerberos environment is called as----------**realm**

18. HMAC stands for----------**hash message authentication code**

19. There are -------number of versions in x.509**3**

20.Version 4 of Kerberos uses ----------encryption mode**cipher block chaining**

UNIT IV

1. Modification user data comes under -----threat.

   a**) integrity** b) confidentiality c) denial of service d) authentication

2. Cryptography checksum is the counter measure of------- threat.

   a)confidentiality b) denial of service c) **integrity** d) authentication

3. Loss of information and loss of privacy are the counter measures of ---- threat.

   a) integrity b) **confidentiality** c) denial of service c) authentication

4. SSL is the security provided at ------level.

   a)network layer b**) transport layer** c) application layer d) preentation layer

5. TLS is the security provided at -----level.

   a).network layer b**) transport layer** c) application layer d) presenttion layer

6. The max fragment block size in SSL is ---

   a) 210 bytes b) 212 bytes c) **214 bytes** d) 216 bytes

7. The major version of SSL is----------

   a) infinite b) zero c) **3** d) 1

8. The minor version of SSL is ----------

   a) infinite b) zero c) 3 d) **1**

9. Handshake protocol uses ----bytes

   a)2 b) 3 c) **4** d) =4

10. The minor version of TLS is ----------

a)infinite b)0 c) 3 d**) 1**

11. ---------- Protocol overcomes the drawbacks of WEP.**WAP**
12. BSS stands for----------**BASIC SERVICE SET**
13. A system used to interconnect a set of BSSs and integrated LANs to create an **ESS**
14. Any device that contains an IEEE 802.11 conformant MAC and physical layer known as----------**STATION**
15. RSN staNEWORK for----------**ROBUST SECURINEWORKORK**
16. The Handshake Protocol consists of a series of messages exchanged by client and server in ----------phases.**SECOND**
17. HTTPS is a combination of --------- and ----------.**HTTP AND SSL/TLS**
18. SSH protocol stack contains ----------.**TLP,UAP,CONNECTION CONTROL**
19. AS stands for----------.**AUTONOMOUS SYSTEM**
20. SSH transport layer protocol provides----------. **STRONG ENCRYPTION ,CRYPTOGRAPHIC HOST AUTHENTICATION AND INTEGRITY PROTECTION**

UNIT-V

1. In PGP services digital signature uses -----algorithms.
   a) DSS/RSA b) RSA/SHA c**) either(a) or (b)** d) DES

2. For message encryption for PGP services --- ----------algorithm is used.
   a) CAST b)IDEA c) Triple ES d) **any of the above**

3. For compression in PGP service -----technique is used.
   a) jar b**) ZIP** c) compresskey d)none of the above
4. In PGP services for email compatibility ------- algorithm is used .
   a) IDEA b) radix-56 conversion c) **radic-64 conversion** d) RSA
5. For message storage transmission ----------function is used.

a**) digital signature** b) e-mail compatibility c) segmentation d) decompression

6. structure of public key ring contains -----no. of fields.
   a) 5 b)**8** c) 7 d) 6
7. Which of the following is not a field of private key ring structure .
   a) timestamp b) Key ID c) **owner trust**d) encrypted private key
8. MIME version parameter value is --------
   a) **1.0** b) 2.0 c) 3.0 d) 4.0
9. S/MIME incorporates ---------- public key algorithms .
   a)2 b)**3** c)4 d) 5
10. S/MIME uses ------algorithm for encrypting session keys.
    a) IDEA b) RSA c) **Diffie-Hellman** d) DES

11. IP Security can be implemented in ---------- mode.**TRANSPORT MODE**
12. Key management facility is used for ---------- layer.**NETWORK LAYER**
13. PGP stands for------ **PRETTY GOOD PRIVACY**
14. IP Security uses ----------routing protocol.**IP**
15. ESP represents ----------**ENCAPSULATING SECURITY PAYLOAD**
16. AH represents ----------**AUTHENTICATION HEADER**
17. Tunnel mode provides protection to ----------**ENTIRE IP PACKET**
18. ---------is the key size allowed in PGP **1024-4096**
19. The key management in IP security is done by_____.**INTERNET KEY EXCHANGE PROTOCOL(IKE)**
20. Nonce is a ----------**NUBER USED ONLY ONCE**