VIGNAN INSTITUTE OF TECHNOLOGY AND SCIENCE
Near Ramoji Film City, Deshmukhi Village, Pochampally Mandal, Yadadri Bhuvanagiri Dist.
(Approved by AICTE, New Delhi, Affiliated to JNTUH, Hyderabad)
Eamcet Code VGNT Dist Code : YBG
AN AUTONOMOUS INSTITUTION

Department of Computer Science & Engineering
Question Bank
IV Year I Semester – 2024-25
CNS DESCRIPTIVE QUESTION BANK

S.No	Descriptive Questions	Marks	CO	PO	BTL
	UNIT-I				
1	a)Differentiate between Plain Text and Cipher Text	2M	1	1	4
	b)Briefly explain about Steganography	3M	1	1	2
	c) Explain with a neat diagram A model for security	5M	1	1	2
	d) Differentiate between Symmetric and Asymmetric Key Cryptography.	5M	1	1	4
2	a)List the principles of security	2M	1	1	1
	b) How security services are related to security mechanisms?	3M	1	1	4
	c) What is steganography? What are the similarities and differences between steganography and cryptography? What are the relative advantages and disadvantages of steganography?	5M	1	2	2
	d) Give the classification of security attacks	5M	1		3
3	a)What is Authentication ?	2M	1	2	1
	b) What is cipher text?	3M	1	1	1
	c) List and briefly explain categories of security services and security mechanisms	10M	1	2	2
4	a) What is cryptanalysis, cryptography?	2M	1	1	1
	b) What are possible types of attacks?	3M	1	2	1

	c) Elaborate any four Substitution techniques and list their merits and demerits.	10M	1	1	2
5	a	2M	1	1	1
	b) Explain key size and key range	3M	1	2	2
	c)) Explain hill cipher with an example	10M	1	1	2
6	a) What is simple columnar technique?	2M	1	1	1
	b) Differentiate between Active attacks and Passive attacks.	3M	1	1	4
	c) Discuss playfair cipher with an example	10M	1	1	2
	UNIT-II				
1	a) What are Symmetric Key Ciphers?	2M	1	1	1
	b) Write a short note on Blowfish algorithm.	3M	1	1,2,3	1
	c) Explain in detail about RC5 algorithm	10M	1	1,2,3	2
2	a) Define Elgamal Cryptography?	2M	1	1,2,3	1
	b) In the RSA system, the public key of a given user is e=31, n=3599. What is the private key of the user?	3M	1	1,2,3	2
	c) With a neat diagram, explain one round of DES algorithm.	5M	1	1,2,3	2
	d) List and explain the principles of public key cryptosystems	5M			2
3	a) Define avalanche effect.	2M	1	1	2
	b) What is the purpose of Diffie-Hellman key exchange?	3M	1	1,2,3	1
	c) Explain RSA encryption. Also, critically analyze the security aspects of RSA.	10M	1	1,2,3	2
4	a) Define linear cryptanalysis	2M	1	1	1
	b) Write about strength of DES algorithm.	3M	1	1,2,3	1
	c) Draw the general structure of DES and describe how encryption and decryption are carried out and identify the strengths of DES algorithm.	10M	1	1,2,3	3
5	a) Compare block ciphers with stream ciphers.	2M	1	1	4
	b) How keys are exchanged in Diffie-Hellman algorithm.	3M	1	1,2,3	1

	c) Apply the mathematical foundations of RSA algorithm. Perform encryption decryption for the following data. P=17, q=7, e=5, n=119, message = "6". Use extended Euclid's algorithm to find the private key.	10M	1	1,2, 3	3
6	a) Define Stream ciphers?	2M	1	1	1
	b) Differentiate conventional & public key encryption.	3M	1	1,2, 3	4
	c) With a neat diagram explain how encryption and decryption are done using Blowfish algorithm?	10M	1	1	2
7	a) Discuss about Electronic code book mode?	2M	1	1,2	2
	b) Do you agree with the statement that an increase in key size of 1 bit doubles the security of DES? Justify your answer.	3M	1	1	3
	c) Give a detailed explanation of key generation and encryption of IDEA algorithm.	10M	1	1,2	2
8	a)Sketch the diagrams for CFB, OFB.	2M	1	1	3
	b) Which of the four different stages involved in each round of AES? Explain it with neat diagrams	3M	1	1	2
	c) Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2. a) If user „A" has public key YA=9, what is A"s private key XA. b) If user „B" has public key YB=3, what is shared secret key K.	10M	1	1	3
UNIT-III					
1	a) Draw the diagram for Symmetric key encryption with confidentiality and authentication	2M	1	1,2	3
	b) Explain Authentication Requirements?	3M	1	1	2
	c) Explain SHA-512 Algorithm in detail	10M	1	1	2
2	a) Define MAC and how it differs from encryption.	2M	1	1,2	1
	b) What are authentication functions and define them briefly.	3M	1	1,2	1
	c) Explain Message Authentication Code (MAC) and Hash function in detail with neat figures.	10M	1	1,2	2
	a) Define Hash function and Digital Signature.	2M	1	1,2	1

	b) Draw the figures of public key encryption a) For confidentiality b) For authentication c) For both confidentiality and authentication.	3M	1	1,2	3
	c)Explain HMAC and CMAC in detail	10M	1	1	2
4	a) What is meant by Symmetric Key Distribution?	2M	2	1	1
	b) Explain Elgamal Digital Signature.	3M	1	1	2
	c) Explain Kerberos version 4 in detail.	10M	2	1	2
5	a) List out approaches for Public Key Distribution.	2M	2	1	1
	b) Write the differences between Kerberos V4 &V5.	3M	2	1	1
	c) Explain X.509 certificates. Give its format	10M	2	1	2
6	a) Discuss the weakness of Public announcement of Public Key Distribution.	2M	2	1	2
	b) Draw the Architecture model of PKI.	3M	2	1	3
	c) Explain Kerberos version5 in detail.	10M	2	1	2
7	a) What is the purpose of X.509 standard?	2M	2	1	1
	b) What problem was Kerberos designed to address? Explain.	3M	2	1	2
	c) Explain digital signatures	5M	1	1	2
	d) Explain secure hash algorithm	5M	1	1,2	2
8	a) What is the job of key distribution center?	2M	1	1	1
	b) Is MAN in the Middle attack possible on SHA-512? Explain.	3M	1	1,2	3
	c) Give the structure of SHA-512 compression function. Explain the structure of each round.	10M	1	1,2, 3	3,2
9	a) List three approaches to message authentication.	2M	1	1,2	1
	b) ;	3M	2	1,2	1
	c) What is HMAC and what are its advantages over MAC?	10M	1	1,2	1
UNIT-IV					
1	a) List out various threats of Web Security.	2M	3	1,2	1
	b) Draw the diagram for Network Level Security approaches.	3M	3	1,2	3

	c) **SSL Handshake Protocol, SSL Change Cipher Protocol, SSL Alert Protocol**	10M	3	1	2
2	a) Differentiate between Http and Https	2M	3	1	4
	b) Explain about SSL Alert protocol	3M	3	1	2
	c) Explain in detail about SSH.	10M	3	1,2	2
3	a) List out the phases of SSL handshake protocol	2M	3	1	1
	b) Explain SSL record protocol operation	3M	3	1,2	2
	c) Explain about HTTPS and TLS	10M	3	1,2	2
4	a) List out the types of satellites.	2M	3	1	1
	b) Explain the issues and challenges in wireless communication.	3M	3	1	2
	c) Explain IEEE 802 protocol architecture	10M	3	1,2	2
5	a) List out IEEE 802.11 services.	2M	3	1,2	1
	b) Brief about IEEE 802.11i scheme pseudorandom function (PRF).	3M	3	1,2	2
	c) Explain IEEE 802.11i RSN services and Protocols	10M	3	1,2	2
6	a) List out IEEE 802 terminologies	2M	3	1,2	1
	b) Explain the differences between wired and wireless LANs	3M	3	1,2	2
	c) Explain IEEE 802.11i Key management phase with neat diagram	10M	3	1,2	2
7	a) What protocols comprise SSL?	2M	3	1	1
	b) Distinguish between an SSL connection and an SSL Session.	3M	3	1	4
	c) Makeup the Security constraints of IEEE802.11i wireless LAN in detail.	5M	3	1,2	3
	d) Compare and Contrast the security threats related to mobile devices.	5M	3	1,2	3
8	a) Define wireless security?	2M	3	1	1
	b) Discuss the mobile device security	3M	3	1	2
	c)List the steps in the SSL record protocol transmission	10M	3	1	1
UNIT-V					

1	a) Define PGP?	2M	4	1	1
	b)What are the principal services provided by PGP?	3M	4	1	1
	c) Explain S/MIME.	5M	4	1	2
	d) Explain Internet key exchange.	5M	4	1	
2	a)How secure inter branch payment transactions are performed?	2M	4	1	1
	b) Write a brief note on Internet Key Exchange.	3M	4	1	2
	c) Give IP security architecture.	5M	4	1	2
	d) Explain anti-replay service in ESP.	5M	4	1	2
3	a)Differentiate between MIME and S/MIME	2M	4	1	4
	b) What is mean by PGP	3M	4	1	1
	c) Briefly explain the scenario of IP security and its Policy.	5M	4	1	2
	d) Explain IP security architecture and also explain basic combinations of security associations with a neat diagram.	5M	4	1	2
4	a) Illustrate the services provided by IPSec.	2M	4	1	3
	b) Describe tunnel mode in IP security	3M	4	1,2	2
	c) List and explain the PGP services and explain how PGP message generation is done with a neat diagram.	10M	4	1,2	2
5	a) What are S/MIME message?	2M	5	1	1
	b) Discuss the basic approaches to building security associations.	3M	5	1	2
	c) Discuss the implementation security features considering secure inter branch payment transactions case study	10M	5	1,2	2
6	a) Explain the reasons for using PGP	2M	4	1,2	2
	b) Draw the IP Security Authentication Header and Identify the functions of each field.	3M	4	1,2	3
	c) Discuss the significance of Key identifiers in a PGP message and describe the 5 header fields in MIME	5M	5	1	2
	d) Explain the Encapsulating Security payload.	5M	5	1,2	2
7	a) Compare Transport mode and Tunnel Mode	2M	5	1,2	4
	b) Explain transport and tunnel modes of ESP.	3M	5	1	2

	c) How does PGP provides confidentiality and authentication service for Email and File storage applications? Draw the Block diagram and elaborate its components	10M	4	1,2	2
8	a) List the different encryption and authentication algorithms used for AH and ESP protocols	2M	5	1,2	1
	b) Outline the applications and benefits of IP Security.	3M	4	1,2	1
	c) What are the principle services provided by s/MIME	5M	5	1,2	1
	d) Explain briefly about Authentication Header.	5M	4	1	2

CNS Objective Questions

UNIT I

Multiple Choice Questions

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 busuiness 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

Fill In The Blanks

11. DOS attacks are caused by_____

12. The process of writing the text as diagonals and reading it as a sequence of rows is known as_____
13. ----------is a technique that facilitates hiding of a message that is to be kept secret inside other messages

14. Science and art of developing cryptosystems is known as----------
15. ----------is the scrambled message or data that is generated as output by encryption algorithm

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

17.----------ensures that only authorized parties are able to modify computer system data and transmitted information
18. A process which is designed to detect, prevent or recover from an attack is known as ------

19.----------means identifying origin of message correctly and it should ensures that identity is not false
20. Any action that compromises the security of data which is owned by an organization is known as ----------

UNIT II

Multiple Choice Questions

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
   (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

Fill In The Blanks

11. In general private key encryption algorithms uses ----- no. of keys.

12. Public key encryption algorithm uses ---- no. of keys .

13. RSA algorithm was developed by---------

14. IDEA stands for---------

15. CBC stands for ----------

16. DES encrypts blocks of ---------- bits

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

18. No of S- boxes used in Blowfish algorithm is ----------

19. There are ----------rounds in Blowfish

20. In ----------one block of plain text is encrypted at a time

UNIT III

Multiple Choice Questions

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 byte
7. SHA -512 uses -----registers
   a) 8 b) 6 c) 4 d)5
8. SHA follows --- format to store values
   a) little enidian 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

Fill In The Blanks

11. SHA represents----------

12. Each block size of SHA -512 is ----------

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

14. TGS stands for----------

15. A ---------- can issue digital certificates

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

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

18. HMAC stands for----------

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

20. Version 4 of Kerberos uses ----------encryption mode

UNIT IV

Multiple Choice Questions

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

Fill In The Blanks

11. ---------- Protocol overcomes the drawbacks of WEP.
12. BSS stands for----------
13. A system used to interconnect a set of BSSs and integrated LANs to create an ____
14. Any device that contains an IEEE 802.11 conformant MAC and physical layer known as----------
15. RSN stands for----------
16. The Handshake Protocol consists of a series of messages exchanged by client and server in ----------phases.

17. HTTPS is a combination of --------- and ----------.
18. SSH protocol stack contains ----------.
19. AS stands for----------.
20.SSH transport layer protocol provides----------.,

UNIT-V

Multiple Choice Questions

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) compress key d)none of the above
4. In PGP services for email compatibility ------- algorithm is used .
   a) IDEA b) radix-56 conversion c) radix-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

Fill In The Blanks

11. IP Security can be implemented in ---------- mode.
12. Key management facility is used for ---------- layer.
13. PGP stands for------
14. IP Security uses ----------routing protocol.
15. ESP represents ----------
16. AH represents ----------
17. Tunnel mode provides protection to ----------
18. ---------is the key size allowed in PGP
19. The key management in IP security is done by_____.
20. Nonce is a ----------