KUMARAGURU
college of technology
character is life

Register Number:……..…

M.E DEGREE EXAMINATIONS: NOV/DEC 2023

(Regulation 2018)

Third Semester

COMMUNICATION SYSTEMS

P18COE0002**:** Communication Network Security

COURSE OUTCOMES

CO1: Classify the symmetric encryption techniques.

CO2: Illustrate various Public key cryptographic techniques.

CO3: Elaborate the network security and web security techniques.

CO4: Outline the various wireless threats.

CO5: Discuss the security in various wireless data networks.

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Assertion (A): RC4 has variable key size and byte oriented operations CO1 [K_2]

   Reason (R): RC4 is widely used stream cipher

   a) Both the statements A and R are individually true but R is not the correct explanation of A
   b) Both the statements A and R are individually true and R is the correct explanation of A
   c) A is true and R is false
   d) Both A and R are false

2. Match the following in AES Standard. CO1 [K_1]

List A	List B
A. Key size D. Round key size	i. 128
B. Expanded key size	ii. 10/12/14
C. Rounds	iii. 128/192/256
D. Round key size	iv. 176/208/240

   a) iv, iii, i, ii.
   b) i, ii, iii, iv.
   c) iii, iv, ii, i.
   d) i, ii, iv, iii.

3. Choose the sequence of steps involved in the following process. CO2 [K_2]
   The steps to perform RSA algorithm is as follows
   1. Determine d such that de = 1mod φ (n)
   2. Select two prime numbers p and q
   3. Select e such that $1<e\leq \varphi(n)$
   4. Calculate φ (n) = (p-1)(q-1)
   5. Calculate n = pq

a) 2, 5, 4, 1, 3 b) 2, 4, 5, 3, 1

c) 2, 4, 5, 1, 3 d) 2, 5, 4, 3, 1

4. Which of the following are the solutions to network security? CO2 [K_2]

i) Encryption ii) Authentication iii) Authorization iv) Non-repudiation

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

c) i, iii and iv only d) All i, ii, iii and iv

5. What is the primary purpose of IP Security in network communication? CO3 [K_2]

a) Compression of IP packets b) Encryption and authentication

c) Routing optimization d) DNS resolution

6. What does the Encapsulating Security Payload (ESP) provide in IPsec? CO3 [K_2]

a) Authentication and encryption b) Access control

c) Decompression d) Compression

7. Eavesdropping is also called as CO4 [K_2]

a) Modification b) Fabrication

c) Interruption d) Interception

8. In the context of network security, what does traffic analysis primarily focus on? CO4 [K_2]

a) Decrypting encrypted data b) Monitoring patterns in communication

c) Identifying malware signatures d) Conducting penetration testing

9. What encryption algorithm is typically used to secure data transmission over GPRS networks? CO5 [K_2]

a) Data Encryption Standard b) Rivest–Shamir–Adleman

c) A5/3 d) Advanced Encryption Standard

10. In GSM, how are the encryption keys generated for securing communication between the mobile device and the network? CO5 [K_2]

a) Public-key cryptography b) SIM card authentication

c) Random number generation d) Pseudo-random algorithms

PART B (10 x 2 = 20 Marks)

11. Outline the blocks and keys used in Triple DES. CO1 [K_2]

12. How confidentiality can be implemented for traffic? CO1 [K_2]

13. In Diffie Hellman protocol g=7,p=23,x=3 and y=5.What is the value of the symmetric key? CO2 [K_3]

14. Define the criteria for a cryptographic hash function. CO2 [K_2]

15. Draw IP security architecture, CO3 [K_1]

16. List the services are provided by Web Security. CO3 [K_1]

17.	Define DOS attack.	CO4	[K_2]
18.	Mention the concept of IP spoofing attack.	CO4	[K_2]
19.	What is the purpose of the SSL handshake phase during a secure connection establishment?	CO5	[K_2]
20.	Highlight a key difference between Wireless transport layer security and Transport layer security	CO5	[K_2]

PART C (10 x 5 = 50 Marks)

21.	Compare symmetric and asymmetric encryption techniques.	CO1	[K_2]
22.	What is design objective of S-box and P-box in encryption algorithm?	CO1	[K_2]
23.	Write a note on key distribution and Management.	CO2	[K_2]
24.	On Elliptic Curve E11(1,6), consider the points G = (2,7) and H = (4,3). Compute 2G and G+H.	CO2	[K_3]
25.	How does the Authentication Header contribute to the security of IP packets?	CO3	[K_2]
26.	Summarize that how do firewalls contribute to web security in a wired network environment.	CO3	[K_2]
27.	Elaborate on cryptographic threats.	CO4	[K_2]
28.	Discuss the challenges and potential solutions in wireless security standard.	CO4	[K_2]
29.	Outline the key components of the WAP security architecture and how do these components work together to ensure secure mobile communication?	CO5	[K_2]
30.	Describe the primary role of a WAP Gateway in the context of mobile communication.	CO5	[K_2]

Answer any TWO Questions

PART D (2 x 10 = 20 Marks)

31.	In AES, the size of the block is same as the size of the round key; in DES, the size of the block is 64 bits, but the size of the round key is 48 bits. What are the advantages and disadvantages of AES over DES with respect to this difference? Which algorithm will you prefer for securing your data? Give your arguments.	CO1	[K_2]
32.	Summarize IP Security in network security.	CO3	[K_2]
33.	Interpret common security vulnerabilities associated with Bluetooth technology.	CO5	[K_2]

****