Register Number:……..

B.E DEGREE EXAMINATIONS: NOV / DEC 2024

(Regulation 2018)

Sixth Semester

ELECTRONICS AND COMMUNICATION ENGINEERING

U18ECE0023**:** Network Security

COURSE OUTCOMES

CO1: Apply block cipher and stream cipher algorithms.

CO2: Employ Public key cryptographic techniques.

CO3: Explain the authentication and hash algorithms.

CO4: Analyze the digital signature concepts and applications.

CO5: Apply the Network and System level security measures.

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

Answer all the Questions:-

PART A (10 x 2 = 20 Marks)

(Answer not more than 40 words)

1.	Encrypt the message “yugam” using Playfair cipher with the keyword ‘COLLEGE’.		CO1	[K_3]
2.	How many rounds does AES-128, AES-192, and AES-256 have, respectively?		CO1	[K_2]
3.	Recall the advantages of public key cryptography over symmetric key cryptography.		CO2	[K_2]
4.	What makes elliptic curve cryptography attractive in constrained environments such as mobile devices or IoT?		CO2	[K_3]
5.	List the requirements for message authentication.		CO3	[K_2]
6.	What are the properties of the hash function in cryptography?		CO3	[K_2]
7.	Differentiate between direct and arbitrated digital signatures.		CO4	[K_2]
8.	List the advantages of the Schnorr digital signature scheme over other signature schemes.		CO4	[K_2]
9.	Outline the role of the X.509 certificate in authentication.		CO5	[K_2]
10.	Summarize the various phases of a computer virus during its lifecycle.		CO5	[K_2]

Answer any FIVE Questions:-

PART B (5 x 16 = 80 Marks)

(Answer not more than 400 words)

11.	a)	Summarize the security attacks and security services defined in OSI architecture standard X.800.	8	CO1	[K_2]
	b)	Explain the encryption and key generation processes of the DES algorithm. With	8	CO1	[K_2]

a neat block diagram.

12.	a)	Outline Diffie-Hellman key exchange algorithm. If Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7. i). If user A has private key $X_A = 5$, Compute A's public key Y_A. ii). If user B has private key $X_B = 12$, Compute B's public key Y_B. iii). Compute the shared secret key K.	8	CO2	[K_3]
	b)	Describe the mathematical foundations of the RSA algorithm. Perform the encryption and decryption for the following: p=17, q=7, e=5, message=”6”.	8	CO2	[K_3]
13.		Define Hash function. Summarize the security features and logic used for the generation of hash code in SHA-512 algorithm. Compare RIPEMD-160 with SHA-512.	16	CO3	[K_3]
14.		Explain the digital signature algorithm and detail the process of signing and verifying messages using the Digital Signature Standard. Also list out the application areas of Digital Signature.	16	CO4	[K_3]
15.	a)	Elaborate the Kerberos authentication protocol, including its key components, authentication process, and role in securing network communication.	8	CO5	[K_3]
	b)	Discuss any two types of firewalls and their roles in enforcing security policies and protecting network resources.	8	CO5	[K_3]
16.	a)	Illustrate the design principle and key schedule of RC4 stream cipher with one example.	8	CO1	[K_3]
	b)	Define Message Authentication Codes (MACs) and explain how they are generated and verified using symmetric cryptographic techniques.	8	CO3	[K_2]

****