Register Number:……………..

KUMARAGURU
college of technology
character is life

B.TECH DEGREE EXAMINATIONS: NOV/DEC 2022

(Regulation 2018)

Fifth Semester

DEPARTMENT OF INFORMATION TECHNOLOGY

U18ITT5002: Cryptography and Network Security

COURSE OUTCOMES

CO1: Explain security attacks and issues in computer systems and networks.
CO2: Apply the mathematics symmetric and asymmetric algorithms related to cryptography
CO3: Explain the purpose and working of authentication and system level security algorithms
CO4: Apply the appropriate security mechanism for different computing environment
CO5: Apply appropriate security methods to solve real life applications

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

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1. Construct a playfair matrix with the key ‘examination’. CO1 [K_3]

2. What do you mean by avalanche effect? CO1 [K_1]

3. What is an elliptic curve? CO2 [K_2]

4. What is the value of 11^4 mod 187? CO2 [K_3]

5. What are the properties of Digital Signature? CO3 [K_3]

6. What do you mean by one way property in hash function? CO3 [K_2]

7. What are the services provided by PGP? CO4 [K_2]

8. What is the difference between TLS and SSL security? CO4 [K_3]

9. What do you mean by Trojan horse? CO5 [K_2]

10. What is Bastion host? CO5 [K_2]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11. a) With the neat diagram explain the algorithm Advanced Encryption Standard in detail. CO2 [K_2]

12. a) Perform encryption and decryption using RSA algorithm for the following. 8 CO2 [K_3]
P =7, q = 11, e = 17, M = 8.

	b)	Users A and B use the Diffie Hellman key exchange technique a common prime q=11 and a primitive root α=5 (i) If user A has private key XA=2, what is A’s public key YA? (ii) If user B has private key XB =3, what is A’s public key YB? (iii)What is the shared secret key?	8	CO2	[K_3]
13.	a)	With the neat diagram explain how secure hash algorithm generates message digest in detail.		CO3	[K_2]
14.	a)	How does PGP provide confidentiality and authentication service for e-mail and storage applications? Draw the block diagram and explain its components.		CO4	[K_2]
15.	a)	Explain in detail about different types of firewalls.	8	CO5	[K_2]
	b)	Explain any two approaches for intrusion detection.	8	CO5	[K_2]
16.	a)	Explain in detail about various types of attacks.	8	CO1	[K_2]
	b)	Describe the various specific security mechanisms	8	CO1	[K_2]

****