Register Number:……………..

KUMARAGURU
college of technology
character is life

B.TECH DEGREE EXAMINATIONS: APRIL / MAY 2023

(Regulation 2018)

Fifth Semester

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. Find the shift row transformation used in AES for the following matrix. CO1 [K_2]

$$\begin{matrix} 45 & 3E & 82 & 21 \\ A7 & 59 & 94 & 4D \\ 3A & 1B & 28 & 73 \\ 3F & 2C & 54 & 62 \end{matrix}$$

2. Construct a Playfair matrix with the key “occurrence”. CO1 [K_3]
3. What do you mean by a trap-door one-way function? CO2 [K_2]
4. State Fermat’s theorem. CO2 [K_2]
5. List any four design goals of HMAC. CO3 [K_2]
6. Specify the requirements for message authentication. CO3 [K_2]
7. Draw the X.509 certificate Format. CO4 [K_3]
8. State the principal services provided by PGP. CO4 [K_3]
9. List the types of intruders. CO5 [K_2]
10. Define Biometric Authentication. CO5 [K_2]

Answer any FIVE Questions:-

PART B (5 x 16 = 80 Marks)

(Answer not more than 400 words)

11.		Give the detailed explanation about DES encryption algorithm.	16	CO1	[K$_2$]
12.	a)	Explain the RSA algorithm in detail. Perform encryption and decryption using RSA Algorithm with p=17, q=31, e=7, M=2.	10	CO2	[K$_3$]
	b)	Illustrate how man-in-the-middle attack happens in Diffie Hellman key exchange protocol.	6	CO2	[K$_2$]
13.		Explain the concepts of SHA-1 in detail with their compression function.	16	CO3	[K$_2$]
14.		How the authentication is ensured using Kerberos, explain with detail dialogue exchanges between server and workstation?	16	CO4	[K$_2$]
15.		Explain about intruders, intrusion techniques and approaches for intrusion detection.	16	CO5	[K$_2$]
16.	a)	ii. Consider a Diffie Hellman scheme with the common prime q=11 and primitive root $\alpha = 2$ (1) Show that 2 is a primitive root of 11. (2) If user A has public key $Y_A = 9$, what is the A's private key X_A? (3) If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A?	6	CO2	[K$_3$]
	b)	Explain the types of firewalls in detail with a neat diagram.	10	CO5	[K$_2$]

****