Register Number:……..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: APRIL / MAY 2023

(Regulation 2018)

Sixth Semester

INFORMATION SCIENCE AND ENGINEERING

U18IST6002: Cryptography and Network Security

COURSE OUTCOMES

CO1: Analyze various security attacks and select appropriate security mechanisms for designing various security services
CO2: Understand the mathematical foundations of cryptography
CO3: Trace the design of modern block ciphers from basic building blocks
CO4: Appreciate how one-way function and other mathematical hard problems are used to construct solutions for message integrity and authentication
CO5: Discover how cryptographic algorithms are used to build network security protocols
CO6: Identify appropriate mechanisms for providing system security

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

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

1.	Differentiate between Brute force Attack and Cryptanalytic Attack with an example each.	CO1	[K4]
2.	Many security protocols make use of symmetric key algorithm for encrypting large messages and then use asymmetric key algorithms for exchanging the symmetric key. What is the reason for preferring symmetric key encryption over asymmetric key encryption for confidentiality in this context?	CO5	[K4]
3.	Which cryptographic algorithm makes use of the hard problem of computing discrete Logarithm?	CO2	[K2]
4.	What is the algorithm that is used to find Modular Multiplicative Inverse?	CO2	[K2]
5.	Identify the name of the Claude Shannon's principle for each of the following: i. Making the relationship between the plain text and key as complex as possible ii. Making the relationship between the cipher text and key as complex as possible	CO3	[K2]
6.	When and Why will you choose to use Triple DES instead of DES, Double DES or AES?	CO3	[K2]
7.	Differentiate between Hash functions and Message Authentication Codes.	CO4	[K2]
8.	Which cryptographic mechanism can assure all of the following: Integrity, Authentication, and sender side non-repudiation?	CO4	[K2]
9.	What is a Phishing Attack? Name any two types of Phishing Attacks.	CO6	[K2]
10.	Differentiate between a Distributed DoS and DoS. Which one is relatively difficult to prevent?	CO6	[K4]

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

11.	a)	The following table has been randomly mapped between Security Attacks, Services and Mechanisms. Order them properly so that it shows for each of the security attacks, what is the security service to be provided using which security mechanism:	8	CO1	[K3]

Security Attacks	Security Services	Security Mechanisms
Interception	Availability	Hash Functions
Fabrication	Integrity	Redundancy
Modification	Authentication	Encryption / Decryption
Interruption	Confidentiality	Message Authentication Code

	b)	Following is the Cipher Text of a primitive cryptographic mechanism. Cryptanalyze or brute force attack and discover the corresponding plain text and explain how you arrived at it. Cipher Text: GEIWEV GMTILV MW IEWC XS FVIEO	8	CO1	[K4]
12.	a)	What is Prime Factorization problem? Explain RSA Key generation steps.	8	CO2	[K2]
	b)	If suppose future quantum computer is able to easily solve prime factorization, analyze how you can discover the private key from the public key of RSA?	8	CO2	[K4]
13.	a)	Explain one round of AES Encryption	8	CO3	[K2]
	b)	Modern Block Ciphers like AES are product ciphers and has a mathematical basis. Justify how AES qualifies to be a product cipher and what is the mathematical foundations and properties based on which AES is built	8	CO3	[K4]
14.	a)	What are the properties that a secure hash function much satisfy?	8	CO4	[K2]
	b)	Show how can a secure hash function like SHA be used to build a Message Authentication Code like HMAC.	8	CO4	[K2]
15.	a)	You need to convert an existing network protocol into a secure network protocol. The requirements are to transmit a large message from a sender to receiver. You need to ensure confidentiality, message integrity, message authentication and sender side nonrepudiation. You also have to handle keys. Design a solution for the above and explain how it addresses the above. You may re-use any aspect of the existing network security protocol for the same.	12	CO5	[K6]
	b)	How will you configure a Virtual Private Network using IPSec?	4	CO5	[K3]
16.	a)	Explain any two approaches to Intrusion Detection Systems	8	CO6	[K2]
	b)	Explain any two types of Firewalls	8	CO6	[K2]

****