Register Number:……..

KUMARAGURU college of technology
character is life

B.E/B.TECH DEGREE EXAMINATIONS: APRIL /MAY 2024

(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 passive attack and active attack. Give example for each type of attack.	CO1	[K_2]
2.	Define cryptanalysis.	CO1	[K_1]
3.	State the use of Primality Test.	CO2	[K_2]
4.	Differentiate between a block cipher and a stream cipher.	CO3	[K_2]
5.	State the purpose of S-Boxes in DES.	CO3	[K_2]
6.	Differentiate Message Authentication Code and Hash function.	CO4	[K_2]
7.	Is the Diffie Hellman key exchange protocol is vulnerable? Justify.	CO4	[K_4]
8.	Outline the properties of Digital Signature.	CO4	[K_2]
9.	List the various ways in which secret keys can be distributed to two communicating parties.	CO5	[K_2]
10.	Define nonce.	CO6	[K_1]

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

11.	a)	Explain about OSI Security architecture model.	10	CO1	[K_2]

	b)	Explain different types of cryptanalytic attacks based on what is known to the attacker.	6	CO1	[K_2]
12.	a)	Using the extended Euclidean algorithm, find the multiplicative inverse of 1234 mod 4321.	10	CO2	[K_3]
	b)	Define Euler's theorem and it's application. Find gcd (1970, 1066) using Euclid's algorithm.	6	CO2	[K_3]
13.	a)	Using the Vigenère cipher, encrypt the word "explanation" using the key leg.	8	CO3	[K_3]
	b)	Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones	8	CO3	[K_3]
14.	a)	Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES. i. XOR of subkey material with the input to the f function ii. XOR of the f function output with the left half of the block iii. f function iv. permutation P v. swapping of halves of the block	10	CO3	[K_4]
	b)	Discuss briefly about meet-in-the-middle attack.	6	CO3	[K_2]
15.	a)	Illustrate about the SHA algorithm and explain.	10	CO4	[K_2]
	b)	Perform encryption and decryption using RSA Algorithm for the following. P=17; q=11; e=7; M=88.	6	CO4	[K_3]
16.	a)	Describe the SSL Architecture in detail. What is the difference between TLS and SSL security?	8	CO5	[K_2]
	b)	What are the services provided by PGP? Explain the reasons for using PGP.	8	CO6	[K_2]

****