3/5/2023

Reg. No.												

Question Paper Code	11833

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL/MAY 2023

Seventh Semester

Computer Science and Engineering

CS8792 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulations 2017)

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks, K-Level, CO
1.	Compare Plain text and Cipher Text.	*2,K2,CO1*
2.	Define Cryptanalysis.	*2,K2,CO1*
3.	Find GCD (1970, 1066) using Euclid's algorithm.	*2,K2,CO2*
4.	Brief about Man in the Middle attack.	*2,K2,CO2*
5.	State Euler's Theorem.	*2,K1,CO3*
6.	Difference between Conventional Encryption and Pubic Key Encryption.	*2,K2,CO3*
7.	Show how SHA is more secure than MD5.	*2,K2,CO4*
8.	Point out any 2 applications of X.509 Certificates.	*2,K2,CO4*
9.	List the steps for preparing envelope data MIME.	*2,K1,CO5*
10.	Describe Trojan Horses.	*2,K2,CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Encrypt the following using play fair cipher using the keyword MONARCHY. Use X for blank spaces "SWARAJ IS MY BIRTH RIGHT".	*13,K3,CO2*
		OR	
	b)	(i) Classify and briefly define types of cryptanalytic attacks based on what is known to the attacker.	*7,K2,CO2*
		(ii) Explain briefly the two general approaches to attacking a cipher.	*6,K2,CO2*
12.	a)	Solve gcd(98,56) using Extended Euclidean Algorithm. Write the algorithm also.	*13,K3,CO3*
		OR	
	b)	Interpret the each of the following elements of DES; indicate the comparable element in AES if available. (i) XOR of sub key material with the input to the function.	*13,K3,CO3*

(ii) F function.
(iii) Permutation p.
(iv) Swapping of halves of the block.

13. a) Explain the key generation, encryption & decryption in Elgamal. *13,K2,CO4*

OR

b) Evaluate Users A and B and use the Diffie Hellman key exchange technique with a common prime q=11 and a primitive root alpha=7. *13,K3,CO4*
(i) If user A has private key X_A =3, what is A's public key Y_A?
(ii) If user B has private key X_B =6, what is B's public key Y_B?

14. a) Compare and contrast the features of SHA-1 and MD-5 algorithm. *13,K2,CO5*

OR

b) (i)What is Kerberos? Explain how it provides authenticated Services. *7,K2,CO*
(ii) Explain the format of the X.509 certificate. *6,K2,CO5*

15. a) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. *13,K2,CO6*

OR

b) Explain how firewalls help in the establishing a security framework for an organization. *13,K2,CO6*

PART - C (1 × 15 = 15 Marks)

16. a) Examine RSA algorithm, perform encryption and decryption to the system with p = 7; q = 11; e = 17; M= 8. *15,K3,CO4*

OR

b) State and prove the Chinese remainder theorem. What are the last two digits of 49^{19}? *15,K3,CO4*