C Reg. No. :

Question Paper Code: 59216

B.E. / B.Tech. DEGREE EXAMINATION, NOV2018

Elective

Computer Science and Engineering

15UCS916-CRYPTOGRAPHY

(Regulation 2015)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 1 = 5 Marks)

1. What is the cipher text of “we will meet” using Caesar cipher? CO1 -R

(a) zhzlppphhp (b) zlzhoophhw (c) zhzloophhw (d) zgzloopggu

2. DES has an initial and final permutation block and___ rounds CO2 -R

(a) 14 (b) 15 (c) 16 (d) 17

3. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text CO3 -R

(a) nlazeiibljji (b) nlazeiibllj ii (c) olaaeiibljki (d) mlaaeiibljki

4. The purpose of Diffie Hellman algorithm is CO4- R

(a) To exchange the key securely (b) To exchange the name of the algorithm

(c) To find GCD (d) To find the largest prime number

5. In tunnel mode IPsec protects the. CO5 -R

(a) Entire IP packet (b) IP header

(c) IP payload (d) None of the these

PART – B (5 x 3= 15Marks)

6. What are the two basic functions used in encryption algorithms? CO1 -R

7. Write briefly about Discrete Logarithm of a number also find gcd (56, 98) using Euclid’s algorithm. CO2 -R

8. Draw the block diagram of one round of DES and write down its strength. CO3 -R

9. What is the role of a compression function in a hash function?. CO4 -R

10. Briefly enumerate the key features of SET services. CO5 -R

PART – C (5 x 16= 80Marks)

11.	(a)	(i) List and explain in detail the different substitution techniques with suitable examples.	CO1 -U	(10)
		(ii) Write short notes on (a) Security Attacks (b)Security Services	CO1 -U	(6)
		Or		

	(b)	(i) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT.
		X=2(mod 3)
		X=3(mod 5)
		X=2(mod 7)
			CO1 -App	(12)

		(ii) State Miller Robin Algorithm to test the Primality?	CO1 -App	(4)
12.	(a)	With a neat sketch, explain about the DES encryption and decryption process with the internal structure.	CO2- App	(16)
		Or		
	(b)	Explain substitute byte transformation and add round key transformation of AES cipher. Write down the evaluation criteria for the same.	CO2- Ana	(16)
13.	(a)	Discuss in detail RSA algorithm, highlighting its computational aspect and security. Perform ecryption and encryption using RSA algorithm with p=17 & q=11 e = 7.M=88 for the message" India is the most developing country in the world"	CO3- Ana	(16)
		Or		
	(b)	Elaborate the different methods of public key distribution systems with suitable diagrams.Vivid how discrete algorithm in the Diffie Hellman key exchange in exchanging the secret key among users with q=353 and α=3 Secret key of A & B are x_A=97, x_B=233 respectively.	CO3- Ana	(16)
14.	(a)	State the requirements for design of an elliptic Curve Crypto System. Using that, explain how secret keys are exchanged and messages are encrypted.	CO4- U	(16)

		Or		
	(b)	Explain SHA-1 processing of a single 512-bit block and also give the single step operation.	CO4- Ana	(16)
15.	(a)	What are the important factors of security in IP networks? Explain the Transport mode and Tunnel mode of security mechanisms in IP security by appending ESP into the Tunnel mode.	CO5- U	(16)
		Or		
	(b)	Sketch the SSL Record format and describe about the services and protocols comprised in SSL Record protocol.	CO5 -U	(16)