C

Reg. No. : | | | | | | | | | | |

Question Paper Code: 59216

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2019

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. A way to improve on the simple mono alphabetic technique is to use different mono alphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is CO1 -R

   (a) Poly alphabetic substitution cipher (b) cryptanalysis

   (c) Poly analysis cipher (d) rail fence cipher

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) nlazeiiblljii

   (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.	Draw the X.21 architecture and explain in detail.	CO1 -R	
7.	Define Diffusion & Confusion.	CO2 -R	
8.	Draw the block diagram of one round of DES and write down its strength.	CO3 -R	
9.	State avalanche effect..	CO4 -R	
10.	Briefly enumerate the key features of SET services.	CO5 -R	

PART – C (5 x 16= 80Marks)

11.	(a)	(i) Explain OSI security architecture model with neat diagram	CO1 -U	(10)
		(ii) Describe the various security mechanisms.	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) The enemy must be stopped at all costs. Do whatever necessary".	CO1 -App	(4)

T	M	P	Q	S
Z	V	W	X	Y
E	O	C	U	R
F	N	A	B	D
L	G	H	I/J	K

12.	(a)	With a neat sketch, explain about the DES encryption and decryption process with the internal structure.	CO2- App	(16)
		Or		
	(b)	Encrypt the message "PAYMOREMONEY" using Hill cipher with the following key matrix. Also explain the hill cipher substitution technique. $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	CO2- Ana	(16)
13.	(a)	Brief out the encryption and decryption process of DES and depict the general structures.	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)	Explain RSA algorithm, perform encryption and decryption for the following message "India is the most developing country in the world" with *p*=7; *q*=11; *e*=17; *M*=8	CO4- U	(16)
		Or		
	(b)	Explain the process of deriving eighty 64-bit words from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19.	CO4- Ana	(16)
15.	(a)	Write the algorithm of MD5 and explain. Compare its performance with SHA-1.	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)