C

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

Question Paper Code: 59216

B.E. / B.Tech. DEGREE EXAMINATION, APRIL 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. In Singular elliptic curve, the equation x^3+ax+b=0 does ____ roots**.** CO3 -R

   (a) does not have three distinct (b) has three distinct

   (c) has three unique (d) has three distinct unique

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. Key distribution often involves the use of _____ which are generated and distributed for temporary use between two parties. CO5 -R

   (a) session keys (b) private key certificates

   (c) public key certificates (d) master keys

PART – B (5 x 3= 15Marks)

6.	What are the two basic functions used in encryption algorithms?	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.	Differentiate MAC and hash function.	CO4 -R	
10.	Explain active and passive attack with example	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) 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) Describe DES algorithm with neat diagram and explain the steps. 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) Explain in detail, the DiffieHellman key exchange. Users A and B use the DiffieHellman key exchange technique, a common prime q=71 and a primitive root α=7 CO3- Ana (16)

1. If user A has private key XA =5, what is A's public key YA?

2. If user B has private key XB =12, what is B's public key YB?

3. What is shared secret key

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 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. CO4- Ana (16)

Show the values of W16, W17, W18 and W19.

15.	(a)	Explain the architecture of IP security in detail.	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)