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

Question Paper Code: 59216

B.E. / B.Tech. DEGREE EXAMINATION, DEC 2020

Elective

Computer Science and Engineering

15UCS916-CRYPTOGRAPHY

(Regulation 2015)

Duration: 1.15 hrs Maximum: 30 Marks

PART A - (6 x 1 = 6 Marks)

(Answer any six of the following questions)

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

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

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

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

4. What is the number of possible 3 x 3 affine cipher transformations? CO2- R

   (a) 168 (b) 840 (c) 1024 (d) 1344

5. 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

6. 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

7. 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

8. For the AES-128 algorithm there are _____ similar rounds and _____ round is different. CO4- R

(a) 2 pair of 5 similar rounds ; every alternate (b) 9 ; the last

(c) 8 ; the first and last (d) 10 ; no

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

(a) Entire IP packet (b) IP header

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

10. When a hash function is used to provide message authentication, the hash function value is referred to as CO5- R

(a) Message Field (b) Message Digest (c) Message Score (d) Message Leap

PART – B (3 x 8= 24 Marks)

(Answer any three of the following questions)

11.	Explain OSI security architecture model with neat diagram	CO1 -U	(8)
12.	With a neat sketch, explain about the DES encryption and decryption process with the internal structure.	CO2- App	(8)
13.	Brief out the encryption and decryption process of DES and depict the general structures.	CO3- Ana	(8)
14.	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	(8)
15.	Write the algorithm of MD5 and explain. Compare its performance with SHA-1.	CO5- U	(8)