C **Reg. No. :** | | | | | | | | | | |

Question Paper Code: 59216

B.E. / B.Tech. DEGREE EXAMINATION, MAY 2018

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. In cryptography, what is cipher? CO1 R

   (a) Algorithm for performing encryption and decryption (b)Encrypted message

   (c) both (a) and (b) (d)None of the mentioned

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

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

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. 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

5. 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 (5 x 3= 15Marks)

6.	What are the two basic functions used in encryption algorithms?	CO1- R	
7.	Define monoalphabetic cipher.	CO2- R	
8.	What is the difference between a block cipher and a stream cipher?	CO3- U	
9.	State avalanche effect.	CO4- R	
10.	What do you mean by one-way property in hash function?	CO5- U	

PART – C (5 x 16= 80Marks)

11.	(a)	(i) Explain OSI security architecture model with neat diagram.	CO1- U	(8)
		(ii) Describe the various security mechanisms.	CO1- U	(8)
		Or		
	(b)	Describe the following substitution techniques in detail. (i) Caesar Cipher (5) (ii) Playfair Cipher (5) (iii) Vigenere Ciphers (6)	CO1- U	(16)
12.	(a)	Write short notes on: (i) Fermat and Euler's theorem (8) (ii) Chinese remainder theorem (8)	CO2- U	(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- App	(16)
13.	(a)	Brief out the encryption and decryption process of DES and depict the general structures.	CO3- U	(16)
		Or		
	(b)	Write about various block cipher modes of operation in detail.	CO3-U	(16)
14.	(a)	Explain AES algorithm with all its round functions in detail.	CO4- U	(16)
		Or		
	(b)	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- App	(16)

15. (a) Explain digital signature standard with necessary diagram in detail. CO5-U (16)

Or

(b) Write the algorithm of MD5 and explain. Compare its performance with SHA-1. CO5-U (16)