SRN | | | | | | | | | | |

PES UNIVERSITY

PES University, Bangalore

(Established under Karnataka Act No. 16 of 2013))

UC16MC525

DEC 2017: END SEMESTER ASSESSMENT
MCA III SEMESTER

UC16MC525 – Cryptography and Network Security

Time: 180 Min | Answer All Questions | Max Marks: 100

1	a)	List and briefly explain categories of passive and active security attacks.	6
	b)	Describe the three key objectives that are at the heart of computer security.	4
	c)	Encrypt the message **" Semester"** using hill cipher K = 5 8 17 3	5
	d)	Using Playfair cipher encrypt the message **" University"** using keyword " college"	5
2	a)	With a neat diagram explain the operations involved in a fiestal network in DES Process	5
	b)	In a DES Algorithm Find the output $S_i(B_i)$ for the DES S-box , i referrers to the output of the i^{th} S box. **(use the given S box table)** 011000 010001 011110 111010 100001 100110 010100 100111	5
	c)	Name the four steps in AES Algorithm. Explain the first two steps briefly.	5
	d)	In an AES Algorithm .Find the missing values of **Mix Columns** Process for the given state.	5

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

State			
D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

=

?	E0	48	28
66	CB	F8	06
?	19	D3	26
E5	9A	7A	4C

P1|3

SRN | | | | | | | | | | |

3	a)	Perform encryption and decryption using the RSA algorithm, for the following. 1. p = 3; q = 11, e = 7; M = 5 2. p = 5; q = 11, e =3; M = 9	6
	b)	Alice and bob use the Diffie–Hellman key exchange with a common prime q=71 and a primitive root a=7. (i) If Alice has private Key X_A= 5, what is A's public key Y_A? (ii) If Bob has private key X_B=12 what is B's public key Y_B? (iii) What is the shared secret key?	5
	c)	What are the principal elements of a public-key cryptosystem?	5
	d)	Find the following values ϕ (231) and ϕ(440)	4
4	a)	List and describe three approaches of attacking RSA.	6
	b)	With a neat diagram explain the use of Hash Function for Message Authentication	6
	c)	What are digital signatures? With a neat diagrams illustrate, how a hash code is used to provide a digital signature.	8
5	a)	Consider a (6,3) linear code whose generator matrix is 1 0 0 1 0 1 0 1 0 1 1 0 0 0 1 0 1 1 Find all code vectors.	6
	b)	List the four means of authenticating user's identity and eexplain Kerberos authentication service.	7
	c)	Define PGP. Explain the operations of PGP.	7