ModelQuestionPaper-1witheffect from2021-22(CBCS Scheme)

USN | | | | | | | | | | |

Seventh Semester B.E.Degree Examination

CRYPTOGRPHY

TIME:03Hours **Max.Marks:100**

Note: 01. Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE**.

		Module-1	*Bloom's Taxonomy Level	COs	Marks
Q.01	a	Define Cryptography & explain symmetric cipher model.	L1,L2	1	7
	b	Explain Ceaser Cipher with example	L2	1	6
	c	Explain Hill Cipher & apply it to encrypt Plain text = paymoremoney with key K= $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$	L3	1	7
		OR			
Q.02	a	Explain working of DES Algorithm with Example	L2	1	10
	b	Explain Play Fair Cipher & Apply its rules for the following Key = MONARCHY Plaintext = CRYPTOGRAPHY to get the cipher text.	L3	1	10
		Module-2			
Q. 03	a	Explain Public key Encryption And Decryption with example.	L2	2	5
	b	Explain the Description of RSA Algorithm .Assume 2prime no as p=3 and q=11 encryption key e =3 apply RSA algorithm & find cipher text for the plaintext m=8 & decrypt the cipher text to obtain plain text	L2,L3	2	10
	c	Explain elliptic curve cryptography algorithm	L2	2	5
		OR			
Q.04	a	Explain Secrecy and Authentication in public key cryptosystem	L2	2	8
	b	Explain diffie Hellman key exchange algorithm with example.	L2	2	7
	c	Explain man in middle attack with example.	L2	2	7
		Module-3			
Q. 05	a	Explain symmetric key distribution using symmetric encryption	L2	3	10
	b	Explain major issues with key distribution center (KDC).	L2	3	10
		OR			
Q. 06	a	Explain symmetric key distribution using asymmetric encryption	L2	3	10
	b	Explain different ways of distributing Public keys	L2	3	10
		Module-4			
Q. 07	a	Explain X.509 CERTIFICATE with format.	L2	4	10
	b	Explain Remote user-authentication using symmetric encryption	L2	4	10
		OR			
Q. 08	a	Explain Kerberos Authentication Service with version 4 Dialogue.	L2	4	10
	b	Explain Remote user-authentication using asymmetric encryption.	L2	4	10
		Module-5			
Q. 09	a	Explain benefits and routing applications of IPSec	L2	5	6
	b	Explain IP security Architecture.	L2	5	6
	c	Explain Security Associations with SA Parameters	L2	5	8

		OR			
Q. 10	a	Explain Authentication Header with figure	L2	5	5
	b	Explain ESP header with figure	L2	5	5
	c	Explain transport mode & Tunnel Mode of IPsec	L2	5	10

REVISEDBLOOMSTAXONOMYLEARNINGLEVEL(RBT)					
L1:Remember	L2:Understand	L3:Apply	L4:Analyze	L5:Evaluate	L6:Create

COURSEOUTCOMES(COs)	
1	Understand Cryptography, Network Security theories, algorithms and systems
2	Apply different Cryptography and Network Security operations on different applications
3	Analyze different methods for authentication and access control
4	Evaluate Public and Private key, Key management, distribution and certification
5	Design necessary techniques to build protection mechanisms to secure computer networks

PROGRAMOUTCOMES(POs)					
1	Engineering Knowledge	5	Modern tool usage	9	Individual and Team-Work
2	Problem Analysis	6	Engineer and Society	10	Communication
3	Design / Development Solutions	7	Environment and Sustainability	11	Project Management and Finance
4	Conduct Investigations of Complex problems	8	Ethics	12	Life-long Learning