[M19 IT 1109]

I M. Tech I Semester (R19) Regular Examinations
PRINCIPLES OF CRYPTOGRAPHY
Department of Information Technology
MODEL QUESTION PAPER

TIME: 3 Hrs.   **Max. Marks: 75 M**

Answer **ONE Question** from **EACH UNIT**
All questions carry equal marks
*****

			CO	KL	M
		UNIT - I			
1.	a).	Identify the classical cryptosystems and its types	1	3	8
	b).	Compare Euler's and Chinese Remainder theorem	1	4	7
		OR			
2.	a).	Distinguish single rnd of DES Algorithm and key discarding process of DES	2	4	8
	b).	Analyze Cauchy 's theorem with example	2	4	7
		UNIT - II			
3.	a).	Distinguish max-flow min-cut theorem	2	4	7
	b).	Apply encryption and decryption for RSA algorithm parameters :p=3, q=11, e=7, d=?, M=5.	2	3	8
		OR			
4.	a).	Identify different types of attacks	1	3	7
	b).	Compare SSL and SET protocols	2	4	8
		UNIT - III			
5.	a).	Distinguish Diffie Hellman key Exchange algorithm with merits and demerits	2	4	8
	b).	Classify Modes of operation in Block cipher	2	4	7
		OR			
6.	a).	Identify different modes of operations in DES	2	3	8
	b).	Identify different Phases, types of virus structure and types of viruses	1	3	7
		UNIT - IV			
7.	a).	Classify fr types of block cipher design	2	4	8
	b).	Analyze the key generation in AES algorithm and its expansion format	3	4	7
		OR			
8.	a).	List t the properties of hash function in cryptography	3	4	7
	b).	Analyze digital signature with ElGamal public key cryptosystem	3	4	8
		UNIT - V			
9.	a).	Distinguish secure hash Algorithm (SHA)	3	4	7
	b).	Compare any two classical crypto systems with suitable examples	1	4	8
		OR			
10.	a).	Classify RSA digital signature	3	4	8
	b).	Compare stream cipher with RC4	3	4	7