(M19CST1109)

I M.Tech I Semester(R19) Regular Examinations
APPLIED CRYPYOGRAPHY
COMPUTER SCIENCE AND ENGINEERING
MODEL QUESTION PAPER

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

Answer ONE Question from EACH UNIT

All questions carry equal marks

			CO	KL	M
		UNIT-1			
1.	a.)	Explain Advanced Protocols	1	1	7
	b.)	Write abt blind signatures and public key cryptography	1	1	8
		OR			
2.	a.)	Classify the block cipher modes of operation	1	1	8
	b.)	Explain block cipher design principles in detail	1	1	7
		UNIT-2			
3.	a.)	State and prove Euler's Theorem and Determine φ(37)and φ(35)	3	2	8
	b.)	Define a Primitive root. Find all primitive roots of 25	3	3	7
		OR			
4.	a.)	Summarize DES encryption algorithm	3	2	8
	b.)	Explain CAST-128 cipher	3	2	7
		UNIT-3			
5.	a.)	Differentiate Sequence generators and Linear Congruential generators	2	1	7
	b.)	Explain stream ciphers using LFSR,RC4	2	1	8
		OR			
6.	a.)	Compare the principle characteristics of MD5,SHA-1	4	2	7
	b.)	Analyze message authentication using MAC	4	2	8
		UNIT-4			
7.	a.)	Perform encryption and decryption using RSA algorithm for p=5,q=11,e=3 and M=9	2	3	7
	b.)	Write about Digital Signature Algorithm	4	2	8
		OR			
8.	a.)	Explain Elliptic Curve Encryption and Decryption	2	2	7
	b.)	Explain RabinmElGamal Algorithm	2	2	8
		UNIT-5			
9.	a.)	Apply Diffie-Hellman algorithm to exchange keys securely	5	2	7

	b.)	With the help of neat diagram ,explain Kerberos action	5	2	8
		OR			
10.	a.)	Write abt the PGP services a)Authentication b)Confidentiality	5	1	8
	b.)	Explain public key cryptography standards	2	1	7