Code No: **RT41051** **R13** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, February - 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B

Answer ALL sub questions from Part-A

Answer any THREE questions from Part-B

*****

PART–A *(22 Marks)*

1.	a)	What is meant by buffer overflow?	[4]
	b)	Explain Cipher Block Chaining Mode.	[4]
	c)	What is Eulers Totient function? Find it for 37 and 21.	[4]
	d)	What is data authentication code?	[3]
	e)	List the transfer encodings used by S/MIME.	[4]
	f)	What is meant by packet sniffing?	[3]

PART–B *(3x16 = 48 Marks)*

2.	a)	Explain the operations, requirements, components of Network security model.	[8]
	b)	What is TCP Session Hijacking? How is it done?	[8]
3.	a)	Give a detailed description of key generation and encryption of IDEA algorithm	[8]
	b)	Explain about CAST-128 encryption algorithm.	[8]
4.	a)	What is discrete logarithm? What are their properties?	[8]
	b)	Using RSA algorithm, Find n, d if p=11, q=3, e=3. Encrypt "HelloWorld" Message.	[8]
5.	a)	Describe HMAC algorithm. Comment on the security of HMAC.	[8]
	b)	Describe signing and verification in Digital Signature Algorithm.	[8]
6.	a)	Write about the usage of session keys, Public and Private keys in PGP.	[8]
	b)	Give the structure of PGP message generation. Explain with a diagram.	[8]
7.	a)	What is meant by Transport mode and tunnel mode? How is authentication header implemented in these two modes?	[8]
	b)	What is rule based Intrusion Detection?	[8]