Code No: **R41051** **R10** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, March - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1	a)	Explain symmetric cipher model with neat block diagram.	[8]
	b)	Explain Confusion and Diffusion in detail.	[7]
2		Explain cipher block modes of operations in detail.	[15]
3	a)	State and prove Eulers' theorem.	[8]
	b)	Use Euler's theorem to find a number x between 0 and 9 such that a is congruent to 6 modulo 35.	[7]
4	a)	Explain RSA algorithm.	[8]
	b)	Perform the encryption and decryption for the following P= 3 ; q=11, e=7,; M=5	[7]
5	a)	What is hash function? Explain the requirements of Hash functions.	[8]
	b)	What is a digital signature? List the requirements of digital signature.	[7]
6	a)	Explain PGP services in detail.	[10]
	b)	What are the limitations of SMTP/822 scheme.	[5]
7	a)	What are the IPSec functional areas? Explain the IPSec key management.	[8]
	b)	Explain the Secure Electronic transaction protocol.	[7]
8	a)	Explain taxonomy of Malicious Software's briefly.	[8]
	b)	What is a firewall? Explain the design goals of firewalls.	[7]