Code No: **R41051** **R10** **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: 75**

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

1	a)	(i)	Write the difference between a block cipher and a stream cipher	
		(ii)	List and briefly define categories of security services.	[8]
	b)		Explain about transportation techniques.	[7]
2	a)		Draw the general structure of DES and explain the encryption-decryption process.	[8]
	b)		Explain the encryption of AES With neat Diagram.	[7]
3	a)	(i)	Determine the gcd (24140,16762) using Euclid's algorithm.	
		(ii)	Discuss about Euler's theorem.	[8]
	b)		Explain the Chinese Remainder theorem.	[7]
4	a)		What are the requirements and applications of public key cryptography? Compare conventional encryption with public key encryption.	[8]
	b)		How do elliptic curves take part in encryption and decryption process?	[7]
5	a)		Describe in detail the overall operation of HMAC algorithm.	[8]
	b)		With neat sketches, discuss the digital signature standard.	[7]
6	a)		Summarize the S/MIME functionality and the cryptographic algorithms used in S/MIME.	[8]
	b)		Give an overview of X.509 certificates and its formats.	[7]
7	a)		Describe the encapsulating security payload of IPSec.	[8]
	b)		Discuss about the SSL architecture.	[7]
8	a)		Explain the various intrusion detection mechanisms.	[8]
	b)		With a neat illustration, discuss the different types of a firewall.	[7]