Code No: I6811/R16

M. Tech. I Semester Regular/Supple Examinations, Jan/Feb-2018

NETWORK SECURITY & CRYPTOGRAPHY

Common to VLSI&ES (68), ES&VLSI (48), VLSID &ES (77), ES &VLSID (81), SSP(45), DIP(63), CE&SP(46), IP(10), C & SP (80), Embedded Systems (55), Digital Systems & Computer Electronics (06), DECS (38), ECE (70), DECE (37), Communication Systems (47)

Time: 3 Hours **Max. Marks: 60**

Answer any FIVE Questions
All Questions Carry Equal Marks

1.	a	Discuss with neat sketch a network security model.	6M
	b	Differentiate passive attack from active attack with example.	6M
2.	a	What is the difference between differential and linear cryptanalysis?	6M
	b	How is expansion permutation function done in DES?	6M
3.	a	Explain the compression of Secure Hash Algorithm.	6M
	b	What are the requirements of hash functions?	6M
4.	a	Describe RIPEMD-160 algorithm in detail and compare its performance with SHA	6M
	b	Write a short note on X.509 directory Authentication service.	6M
5.	a	Explain the architecture of IP security and mention the benefits and services of it.	6M
	b	Differentiate Secure sockets layer from Secure Electronic Transaction.	6M
6.	a	Explain in detail about various types of attacks.	6M
	b	Write short notes on Steganography and mention the advantages of Steganography over cryptography .	6M
7.	a	Define virus? Briefly explain the phases of virus	6M
	b	Describe the Fire wall Design Principles in detail	6M
8.	a	With the help of example explain Euclid's Algorithm	6M
	b	With the help of example explain Modular arithmetic theorem	6M

*****

|'''|||||''|'''|||||