Ref No: EX/PG/DMC/T/128A/2018

M. Tech. Distributed & Mobile Computing Examination, 2018

(1st year) (1st / 2nd Semester/~~Repeat/Supplementary/Annual/Bi-Annual~~)

SUBJECT: - Security in Wireless and Mobile Systems

Time: ~~Two hours~~/Three hours/ ~~Four hours~~/ ~~Six hours~~ Full Marks: 100

No. of Questions	Answer any *five* questions.	Marks
1.	a) What are the characteristics of network security?	6
	b) Differentiate between virus and worms. Explain the various phases of virus life cycle.	3+3
	c) Differentiate between MAC and Hash.	4
	d) Distinguish between public and private key.	4
2.	a) Explain overall structure of S-DES with help of diagram. Explain role of sub key generation with suitable analysis.	6+5
	b) In S-DES 10 bit key given is 1000100010.Find the sub keys K1 and K2 if :	6
	i. P10 = 3 5 2 7 4 10 1 9 8 6	
	ii. P8 = 6 3 7 4 8 5 10 9	3
	c) What is avalanche effect?	8
3.	a) Explain one round of MD5 operation.	6
	b) Compare MD5 with SHA.	6
	c) Discuss the advantages and disadvantages of HMAC.	
4.	a) How does SSL work? Explain in details.	10
	b) What are the services offered by PEM? Explain the working of PEM.	6
	c) Explain in context of SET the function of dual signature.	4
5.	a) Explain the various fields of Encapsulating Security Payload (ESP) packet.	5
	b) How IP security implemented in transport mode?	3
	c) What service does handshake protocol of SSL provide? How does the handshake protocol of SSL work?	4+4
	d) What are the additional enhancements that are being provided in TLS?	4
6.	a) Explain the WAP architecture. How is communication between WAP client and Web server done?	3+3
	b) Why do we need WTLS? How does it provide security?	4+4
	c) Explain one round of S-DES?	6
7.	Write short note on :	5x4
	a) Screened host firewall.	
	b) NAT	

M. Tech. Distributed & Mobile Computing Examination, 2018

(1st year) (~~1st~~ / 2nd Semester/~~Repeat/Supplementary/Annual/Bi-Annual~~)

SUBJECT: - Security in Wireless and Mobile Systems

Time: ~~Two hours~~/Three hours/ ~~Four hours~~/ ~~Six hours~~ Full Marks: 100

c) CBC mode
d) RSA algorithm
e) Poly alphabetic cipher.