Ref No: EX/PG/DMC/T/128A/2019

M. Tech. Distributed & Mobile Computing Examination, 2019

(1st year) (1st / 2nd Semester/I

SUBJECT: - Security in Wireless and Mobile Systems

Time: Three hours/ Full Marks: 100

No. of Questions	Answer any *five* questions.	Marks
1.	a) What are the principles of network security?	6
	b) Differentiate between active and passive attack. Explain masquerade attack.	4+3
	c) What are the requirements of public key cryptography?	3
	d) Distinguish between symmetric and asymmetric key cryptography.	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 : i. P10 = 3 5 2 7 4 10 1 9 8 6 ii. P8 = 6 3 7 4 8 5 10 9	6
	c) What is avalanche effect?	3
3.	a) What are the services provided by PGP? Explain the working of PGP.	3+4
	b) State reasons of having Dual Signature in SET. Describe how Dual signature is generated & how it achieves its intended goal.	5
	c) Explain in context of SET function of digital envelope.	4
	d) Briefly describe the different phases in Payment Processing session in SET.	4
4.	a) What is packet filtering router? What are the main actions of packet filter router?	3+3
	b) How is Screened host firewall, Dual – homed Bastion different from Screened host firewall, Single homes bastion?	4
	c) What is significance of tunnel mode?	4
	d) How does NATing helps in security of message?	6
5.	a) What is WAP? Why is it being used?	
	b) Explain the WAP stack structure .How is the communication between the WAP client and WAP server done?	3+3 5+3
	c) What are the goals of WTLS and how does it provide security?	3+3
6.	a) What are the benefits provided by IPSec?	
	b) What are AH and ESP and how do they provide transport and tunnel mode of operations?	6 3+4
	c) How does AH deal with replay attack?	
	d) Explain the working of PGP.	3 4

Ref No: EX/PG/DMC/T/128A/2019

M. Tech. Distributed & Mobile Computing Examination, 2019

(1st year) (1st / 2nd Semester/

SUBJECT: - Security in Wireless and Mobile Systems

Time: Three hours/ Full Marks: 100

7.	Write short note on: a) DMZ b) MD5 c) 1 round of IDEA d) Defiee -Hellman key exchange algorithm e) CFB mode f) Digital Signature.	20