Code No: J2503/R16

M. Tech. II Semester Regular Examinations, May-2017

CYBER SECURITY

(Common to Software Engineering (25), Information Technology (40),Computer Science (05) Computer Science & Engineering (58)

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

Answer any FIVE Questions
All Questions Carry Equal Marks

1.	a	Consider a desktop publishing system used to produce documents for various organizations. i) Give an example of a type of publication for which confidentiality of the stored data is the most important requirement. ii) Give an example of a type of publication in which data integrity is the most important requirement. iii) Give an example in which system availability is the most important requirement.	8M
	b	Give a brief note on man-in-the-middle attacks.	4M
2.	a	What are the HMAC design objectives as per the RFC’s? Explain.	6M
	b	Explain any two approaches of Message Authentication.	6M
3.	a	Use Fermat's Theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29.	8M
	b	What is digital signature? Explain the benefits of digital signature.	4M
4.	a	In PGP, can an e-mail message use two different public key algorithms for encryption and signing? How is this defined in a message sent from Alice to Bob?	6M
	b	Discuss how SSL record protocol provides confidentiality and message integrity for SSL connections?	6M
5.	a	Consider any commercial hardware firewall and explain it in detail.	8M
	b	What are the different intrusion detection techniques? How to prevent false alarms in IDS?	4M
6.	a	Give the classification of security attacks. How security services are related to security mechanisms?	6M
	b	How discrete logarithms are used in ELGAMAL algorithm? Explain.	6M
7.	a	Select any three antivirus of your choice and explain their features.	8M
	b	What are the roles of the Oakley key determination protocol and ISAKMP in IPsec?	4M
8.	a	Discuss the Secure Hash Function Algorithm in detail.	6M
	b	Explain the X.509 V3 certificate format.	6M

*****