CSE4003	CYBER SECURITY	L	T	P	J	C
		3	0	0	4	4
Pre-requisite	**Nil**	**Syllabus version**				
		v1.0				

Course Objectives:

1. To learn the concepts of number theory, cryptographic techniques.
2. To understand integrity and authentication process.
3. To familiarize various cyber threats, attacks, vulnerabilities, defensive mechanisms, security policies and practices.

Expected Course Outcome:

1. Know the fundamental mathematical concepts related to security.
2. Implement the cryptographic techniques to real time applications.
3. Comprehend the authenticated process and integrity, and its implementation
4. Know fundamentals of cybercrimes and the cyber offenses.
5. Realize the cyber threats, attacks, vulnerabilities and its defensive mechanism.
6. Design suitable security policies for the given requirements.
7. Exploring the industry practices and tools to be on par with the recent trends

Student Learning Outcomes (SLO):	**1,5,9**

Module:1	**Introduction to Number Theory**	**6 hours**

Finite Fields and Number Theory: Modular arithmetic, Euclidian Algorithm, Primality Testing: Fermats and Eulers theorem, Chinese Reminder theorem, Discrete Logarithms

Module:2	**Cryptographic Techniques**	**9 hours**

Symmetric key cryptographic techniques: Introduction to Stream cipher, Block cipher: DES, AES,IDEA Asymmetric key cryptographic techniques: principles,RSA,ElGamal,Elliptic Curve cryptography, Key distribution and Key exchange protocols.

Module:3	**Integrity and Authentication**	**5 hours**

Hash functions,Secure Hash Algorithm (SHA)Message Authentication, Message Authentica- tion Code (MAC), Digital Signature Algorithm : RSA ElGamal based

Module:4	**Cybercrimes and cyber offenses**	**7 hours**

Classification of cybercrimes, planning of attacks, social engineering:Human based, Computer based: Cyberstalking, Cybercafe and Cybercrimes

Module:5	**Cyber Threats, Attacks and Prevention**	**9 hours**

Phishing, Password cracking, Keyloggers and Spywares, DoS and DDoS attacks, SQL Injection Identity Theft (ID) : Types of identity theft, Techniques of ID theft

Module:6	**Cybersecurity Policies and Practices**	**7 hours**

What security policies are: determining the policy needs, writing security policies, Internet and email security policies, Compliance and Enforcement of policies, Review

Module:7	**Recent Trends**	**2 hours**

	Total Lecture hours:	**45 hours**	

Text Book(s)	
1.	Cryptography and Network security, William Stallings, Pearson Education, 7th Edition, 2016
2	Cyber Security, Understanding cyber crimes, computer forensics and legal perspectives, Nina Godbole,Sunit Belapure, Wiley Publications, Reprint 2016
3	Writing Information Security Policies, Scott Barman, New Riders Publications, 2002
Reference Books	
1.	Cybersecurity for Dummies, Brian Underdahl, Wiley, 2011
2.	Cryptography and Network security, Behrouz A. Forouzan , Debdeep Mukhopadhyay, Mcgraw Hill Education, 2 nd Edition, 2011

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar			
Recommended by Board of Studies	04-04-2014		
Approved by Academic Council	No. 37	Date	16-06-2015