

INFORMATION SECURITY

VIII Semester: CSE / IT								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
ACS013	Core	L	T	P	C	CIA	SEE	Total
		3	-	-	3	30	70	100
Contact Classes: 45		Tutorial Classes: Nil		Practical Classes: Nil		Total Classes: 45		
I. COURSE OVERVIEW:								
<p>This course focuses on the fundamentals of security that are used in protecting both the information present in computer storage as well as information passing over any computer networks. It includes attacks, security mechanisms, and secret-key and public-key cryptography. The authentication protocols and key management techniques for providing security in Email, IP and web, Firewalls and virtual private networks are learned.</p>								
II. OBJECTIVES:								
The course should enable the students to:								
<p>I Understand security standards and practices. The scope and essentiality of threats, attacks to computers and networks associated to them</p> <p>II The symmetric and asymmetric key generation techniques used for providing message authentication, confidentiality and Integrity</p> <p>III The use cases on cryptography and security systems for server and client systems such as web, email and firewalls</p>								
III. COURSE OUTCOMES:								
After successful completion of the course, students should be able to:								
CO 1	Outline model for network security and cryptographic algorithms to prevent attacks on computer and computer security.							Understand
CO 2	Demonstrate symmetric and asymmetric key ciphers for messaging end to end encryption used in different types of cryptographic algorithms							Understand
CO 3	Make use of tools and protocols used in message authentication and hashing functions for every day computing to remain secure							Apply
CO 4	Choose appropriate architecture and protocols used in email and IP security to protect against attackers and intruders							Apply
CO 5	Select firewalls to provide web security as case study in cryptography and network security							Apply
CO 6	Utilize cryptographic and security algorithms to enhance defense against cyber attacks and to improve organization working culture.							Apply
IV. SYLLABUS:								
UNIT-I	ATTACKS ON COMPUTERS AND COMPUTER SECURITY						Classes: 08	
<p>Attacks on computers and computer security: Introduction, the need for security, security approaches, principles of security, types of security attacks, security services, security mechanism, a model for network security; Cryptography concepts and techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.</p>								
UNIT-II	SYMMETRIC KEY CIPHERS						Classes: 10	
<p>Symmetric key ciphers: Block cipher principles and algorithms (DES, AES, Blowfish), differential and linear cryptanalysis, block cipher modes of operation, stream ciphers, RC4 location, and placement of encryption function, key distribution; Asymmetric key ciphers: Principles of public key cryptosystems, algorithms (RSA Diffie - Hellman, ECC) key distribution.</p>								

UNIT-III	MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS	Classes: 08
<p>Message authentication algorithm and hash functions: Authentication requirements, functions, message, authentication codes, hash functions, secure hash algorithm, whirlpool, HMAC, CMAC, digital signatures, knapsack algorithm.</p> <p>Authentication application: Kerberos, X.509 authentication service, public – key infrastructure, biometric authentication.</p>		
UNIT-IV	E-MAIL SECURITY	Classes: 10
<p>E-mail Security: Pretty Good Privacy; S/MIMI IP Security: IP security overview, IP security architecture, authentication header, encapsulating security payload, combining security associations, key management.</p>		
UNIT-V	WEB SECURITY	Classes: 09
<p>Web security: Web security considerations, secure socket layer and transport layer security, secure electronic transaction intruders; Virus and firewalls: Intruders, intrusion detection password management, virus and related threats, countermeasures, firewall design principles; Types of firewalls Case Studies on Cryptography and security: Secure inter-branch payment transactions, cross site scripting vulnerability, virtual electronics.</p>		
Text Books:		
<ol style="list-style-type: none"> 1. William Stallings, “Cryptography and Network Security”, Pearson Education, 4th Edition, 2005. 2. Atul Kahate, “Cryptography and Network Security”, McGraw-Hill, 2nd Edition, 2009. 		
Reference Books:		
<ol style="list-style-type: none"> 1. C K Shymala, N Harini, Dr. T R Padmanabhan, “Cryptography and Network Security”, Wiley India, 1st Edition, 2016. 2. Behrouz A. Forouzan Debdeep Mukhopadhyay, “Cryptography and Network Security”, McGraw-Hill, 2nd Edition, 2010. 		
Web References:		
<ol style="list-style-type: none"> 1. http://bookboon.com/en/search?q=INFORMATION+SECURITY 2. https://books.google.co.in/books/about/Cryptography_Network_Security_Sie_2E.html?id=Kokjwdf0E7QC 3. https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C 		
E-Text Books:		
<ol style="list-style-type: none"> 1. https://books.google.co.in/books/about/Information_Security.html 2. http://www.amazon.in/Cryptography-Network-Security-Behrouz-Forouzan/dp/007070208X 		
Course Home Page:		