CRYPTOGRAPHY AND NETWORK SECURITY

V Semester: IT

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
AITC11	Core	3	1	0	4	30	70	100
Contact Classes: 45	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 45		

Prerequisites: Computer Networks

I. COURSE OVERVIEW:

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 virtualprivate networks are learned.

II.COURSE OBJECTIVES:

The students will try to learn:

I. The security standards and practices. The scope and essentiality of threats, attacks to computers and networks associated to them
II. The symmetric and asymmetric key generation techniques used for providing message authentication, confidentiality and Integrity
III. The Usecases on cryptography and security systems for server and client systems such as web, email and firewalls.

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO 1	**Outline** dmodel 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 ofcryptographic algorithms	Understand
CO 3	**Make use of** tools and protocols used in message authentication and hashing functions for every day computing to remine 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 incryptography and network security	Apply
CO 6	**Utilize** cryptographic and security algorithms to enhance defence against cyber attacks and to improve organization working culture.	Apply

IV. COURSE SYLLABUS:

MODULE – I: ATTACKS ON COMPUTERS AND COMPUTER SECURITY (09)

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.

MODULE – II: SYMMETRIC KEY CIPHERS (10)

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.

MODULE – III: MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS (10)

Message authentication algorithm and hash functions: Authentication requirements, functions, message, authentication codes, hash functions, secure hash algorithm, whirlpool, HMAC, CMAC, digital signatures, knapsack algorithm.

Authentication application: Kerberos, X.509 authentication service, public – key infrastructure, biometric authentication.

MODULE – IV:E-MAIL SECURITY (07)

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.

MODULE – V: CONNECT TO AN EXTERNAL API (09)

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.

V.TEXT BOOKS:

1. William Stallings, "Cryptography and Network Security", Pearson Education, 7th Edition, 2017.
2. Atul Kahate, "Cryptography and Network Security", McGraw-Hill, 4th Edition, 2019.

VI. REFERENCE BOOKS:

1. C K Shymala, N Harini, Dr. T R Padmanabhan, "Cryptography and Network Security", Wiley India, 1st Edition, 2016.
2. Behrouz A. ForouzanDebdeep Mukhopadhyay, "Cryptography and Network Security", McGraw- Hill, 2nd Edition, 2010.

VII. WEB REFERENCES:

1.http://bookboon.com/en/search?q=INFORMATION+SECURITY
2.https://books.google.co.in/books/about/Cryptography_Network_Security_Sie_2E.html?id=Kokjwdf0E7Q C
3.https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C