INFORMATION SECURITY

VIII Semester: CSE / IT

Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
ACS013	Core	3	1	-	4	30	70	100
Contact Classes: 45	Tutorial Classes: 15	Practical Classes: Nil				Total Classes: 60		

OBJECTIVES:

The Students Will Try To Learn:

I Understand 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 use cases on cryptography and security systems for server and client systems such as web, email and firewalls.

COURSE OUTCOMES:

After successful completion of the course, Students will be able to:

CO 1 **Identify computer and networks security threats and classify the threats for prevent, detect and recover from the attacks.**

CO 2 **Explain Encryption and decryption mechanism using block and stream ciphers.**

CO 3 **Summarize key distribution and random generation technique for message authentication.**

CO 4 **Demonstrate the symmetric and asymmetric key ciphers principles and algorithms.**

CO 5 **Use stream or block ciphers algorithms for message authentication.**

CO 6 **Use hashing technique for finding data integrity threats and modification attacks on the data.**

CO 7 **Develop a cryptosystem using digital signatures for exchanging an encrypted message with confidentiality.**

CO 8 **Outline the authentication application in distributed ,biometric and digital certificates for user, computer or service.**

CO 9 **Explain procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise.**

CO10 **Recognize the need of intrusion detection or prevention mechanisms.**

CO11 **Solve unauthorized access from the internet by using firewalls design principles according network structure of the organization.**

CO12 **Explain use cases on cryptography and security systems for real time transactions and finding vulnerabilities and virtual electronics.**

UNIT -I	ATTACKS ON COMPUTERS AND COMPUTER SECURITY	Classes: 10

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.

UNIT -II	SYMMETRIC KEY CIPHERS	Classes: 08

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.

UNIT -III	MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS	Classes: 09

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.

UNIT -IV	E-MAIL SECURITY	Classes: 08

E-mail Security: Pretty Good Privacy; S/MIME IP Security: IP security overview, IP security architecture, authentication header, encapsulating security payload, combining security associations, key management.

UNIT-V	WEB SECURITY	Classes: 10

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.

Text Books:

1 William stallings, " Cryptography and Network Security", pearson Education, 4th Edition,2005.
2 Atulkahate, "Cryptography and Network Security" Pearson McGraw-Hill, 2nd Edition, 2009.

Reference Books:

1 C K Shymala, N Harini, Dr. T R Padmanabhan, "Cryptography and Network Security", Wiley India, 1st Edition, 2016.
2 Behrouz A. ForouzanDedeepMukhopadhyay, "Cryptography and Network Security", McGrawHill, 2nd Edition, 2010.

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= Kokjwdf0E7QC
3. https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C

E-Text Books:

1. https://books.google.co.in/books/about/Information_Security.html
2. http://www.amazon.in/Cryptography-Network-Security-BehrouzForouzan/dp/007070208X