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: 15**	**Practical Classes: Nil**				**Total Classes: 60**		

OBJECTIVES:

The course should enable the students to:

I. Learn the basic categories of threats to computers and networks.
II. Understand various cryptographic algorithms and be familiar with public-key cryptography.
III. Apply authentication functions for providing effective security.
IV. Analyze the application protocols to provide web security.
V. Discuss the place of ethics in the information security area

COURSE OUTCOMES:

1. Understand the basic concepts on attacks of computer ,computer security.
2. Understand the concepts of symmetric key ciphers.
3. To describe about the message authentication algorithm and hash functions.
4. Understand the concepts of e-mail security.
5. Understand the concepts of web security

COURSE LEARNING OUTCOMES:

1. Understand the different types of attacks, security mechanisms, security services.
2. Explain various substitution techniques such as play-fair cipher, mono-alphabetic cipher and hill cipher.
3. Understand various Transposition techniques such as row transposition and rail-fence.
4. Describe the role of private and public key in encryption and decryption and key size.
5. Apply the symmetric algorithm for message transmission and analyze the security level of it.
6. Understand various asymmetric key encryption algorithms for message encryption and decryption.
7. Understand the block cipher modes of operation for encryption and decryption.
8. Describe the need of stream ciphers in message encryption.
9. Understand the role of elliptic curve cryptography in security.
10. Analyze the drawbacks of RSA and able to design a security algorithm which overcomes that drawbacks.
11. Explain the role of the message authentication in message transmission.
12. Explain the need of digital signature in message transmission.
13. Explain and demonstrate the role of different types of hash functions for providing security.
14. Understand the differences between the symmetric and symmetric cryptography algorithms for providing security.
15. Explain S/MIME and PGP for transmitting mail from sender to receiver.
16. Explain IP security for internet protocol and analyze how it provides security.
17. Describe the security socket layer and transport layer security for web security.
18. Demonstrate various types of intrusion detection techniques.
19. Understand various types of viruses and its vulnerabilities.
20. Describe various types of firewalls and analyze the security levels of these.

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 Book:

1. William Stallings, “Cryptography and Network Security”, Pearson Education, 4th Edition, 2005.
2. AtulKahate, “Cryptography and Network Security”, 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.
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

2 http://www.amazon.in/Cryptography-Network-Security-BehrouzForouzan/dp/007070208X