B.Tech.III Year ISem.

CY3101PC: INFORMATION SECURITY

III-I:CSE(CS)								
Course Code	**Category**	**Hours/Weak**			**Credits**	**Max Marks**		
CY3101PC	**Core**	**L**	**T**	**P**	**C**	**CIE**	**SEE**	**Total**
		3	**0**	**0**	**3**	**25**	**75**	**100**
Contact Classes:45	**Tutorial classes:15**	**Practical classes: Nill**				**Total Classes:60**		
Prerequisites								

Course Objectives:

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.
- Discuss Web security and Firewalls

Course Outcomes:

- Studentwillbeabletounderstandbasiccryptographicalgorithms,messageandwebauthenticationand security issues.
- Abilitytoidentifyinformationsystemrequirementsforbothofthemsuchasclientandserver.
- Abilitytounderstandthecurrentlegalissuestowardsinformationsecurity.

UNIT-I

SecurityConcepts: Introduction,Theneedforsecurity,Securityapproaches,Principlesofsecurity,Types of Security attacks, Security services, Security Mechanisms, A model for Network Security**CryptographyConceptsandTechniques:**Introduction,plaintextandciphertext, substitutiontechniques,transpositiontechniques,encryptionanddecryption,symmetricandasymmetrickeycryptography,steganography,key range and key size, possible types of attacks.

UNIT-II

SymmetrickeyCiphers: BlockCipherprinciples,DES,AES,Blowfish,RC5,IDEA,Blockcipheroperation,Streamciphers,RC4.

AsymmetrickeyCiphers: Principlesofpublickeycryptosystems,RSAalgorithm,ElgamalCryptography,Diffie-HellmanKey Exchange, Knapsack Algorithm.

UNIT-III

CryptographicHashFunctions: MessageAuthentication,SecureHashAlgorithm(SHA-512),**Message authentication codes:** Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & AsymmetricEncryption,DistributionofPublicKeys,Kerberos,X.509AuthenticationService,Public–KeyInfrastructure

UNIT-IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH)

Wireless Network Security:

WirelessSecurity,MobileDeviceSecurity,IEEE802.11WirelessLAN,IEEE802.11iWirelessLAN Security

UNIT-V

E-

MailSecurity: PrettyGoodPrivacy,S/MIME**IPSecurity:**IPSecurityoverview,IPSecurity architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange

Case Studies on Cryptography and security : Secure MultipartyCalculation,VirtualElections,SinglesignOn,SecureInter-branchPaymentTransactions,CrosssiteScripting Vulnerability.

TEXTBOOKS:

1. Cryptography and Network Security-Principles and Practice: WilliamStallings,PearsonEducation,6th Edition
2. Cryptography and Network Security:AtulKahate,McGrawHill,3rd Edition

REFERENCEBOOKS:

1. CryptographyandNetworkSecurity:CKShyamala,NHarini,DrTRPadmanabhan, WileyIndia,1st Edition.
2. Cryptography and Network Security:ForouzanMukhopadhyay,McGrawHill,3rd Edition
3. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM. Arthur Conklin ,Greg White, TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning
6. Network Security and Cryptography :Bernard Menezes, CENGAGE Learning