Vidyavardhaka Sangha®, Mysore
VIDYAVARDHAKA COLLEGE OF ENGINEERING
Autonomous Institute, Affiliated to Visvesvaraya Technological University, Belagavi
(Approved by AICTE, New Delhi & Government of Karnataka)
Accredited by NBA | NAAC with 'A' Grade
Department of Information Science & Engineering
Phone: +91 821-4276210, Email: hodis@vvce.ac.in
Web: http://www.vvce.ac.in
@vvceofficial

SEMESTER – V

Course Name:	**Cryptography & Network Security**	**Course Code:**	21IS552
No. of Lecture Hours / Week:	**03**	**CIE Marks:**	**50**
No. of Practical Hours / Week:	**00**	**SEE Marks:**	**50**
Total No. of Lecture + Tutorial / Practical Hours :	**40 + 00 = 40**	**SEE Duration:**	**3 Hrs.**
L:T:P:	**3:0:0**	**CREDITS:**	**03**

Prerequisite:
Basic knowledge of computer networks and security attacks.

Course Overview:
Cryptography and network security is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analysing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Course Learning Objectives (CLO):
- To understand the basic concepts of network security.
- Illustrate key management issues and solutions.
- To develop various security algorithms.

MODULES	TEACHING HOURS
MODULE 1 Classical encryption techniques: Symmetric Cipher Model, substitution ciphers and transposition ciphers, cryptanalysis, Rotor Machines, steganography, Traditional Block Cipher Structure. Block Ciphers and Data Encryption Standard: The Data Encryption Standard, The Strength of DES, Block Cipher Design Principle **SLT:** Shannon's theory of confusion and diffusion. **Textbook:** Ch.2 and 3	8
MODULE 2	8

Public Key Cryptography and RSA: Principals of public key crypto systems, RSA algorithm, security of RSA. Other Public Key Cryptosystem: Diffie-Hellman Key Exchange, Key Exchange Protocols, Man-in-the-Middle Attack. **SLT:** PRNG Based on RSA **Textbook:** Ch.9.1,9.2,10.1	
MODULE 3 Cryptographic Hash Functions: Applications of Cryptographic Hash Function. Message Authentication Codes: Authentication requirements, authentication functions, message authentication code. Digital Signatures: Digital Signatures, Elgamal Digital Signature Techniques. **SLT:** Proof of digital signature algorithm. **Textbook:** Ch.11.1,12.1,12.2,12.3,13.1,13.2	8
MODULE 4 Key Management and distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, Public-Key Infrastructure. User Authentication**:** Kerberos. **SLT :** X.509 Certificates **Textbook:** Ch.14.1,14.2,14.3,14.5,15.3	8
MODULE 5 Electronic Mail Security**:** Pretty Good Privacy, S/MIME IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations. **SLT:** Internet Key Exchange **Textbook:** Ch 19.1,19.2,20.1,20.2,20.3,20.4	8
Textbook 1. William Stallings, "Cryptography and Network Security: Principals and Practice", Pearson Education, 6th Edition, 2014	
Reference Books 1. Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition. 2. Cryptography and Network Security- Behrouz A Forouzan, Debdeep Mukhopadhyay, Mc-GrawHill, 3rd Edition, 2015	
COURSE OUTCOMES (COs)	

At the end of the course, students will be able to	
CO1	**Understand** the need of security and various encryption techniques
CO2	**Apply** the use of public key crypto system to authenticate the messages.
CO3	**Analyse** the digital signature standards and IP security policies.
CO4	**Demonstrate** the various Security Algorithms for a given problem in a team.

CO – PO – PSO Matrix:

	PO1	PO2	PO3	PO4	P05	P06	P07	P08	P09	PO10	P011	P012	PS01	PSO2	PS03	PS04
CO1	2															
CO2	3															
CO3		2														
CO4						2										2
Avg.	2.5	2				2										2