CP308: INFORMATION SECURITY
CREDITS = 5 (L=3, T=0, P=2)

Course Objective:
To impart basic knowledge of Cryptography, Information Security and Cyber Security.

Teaching and Assessment Scheme:

Teaching Scheme			Credits	Marks Distribution				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE	CE	ESE	CE	
3	0	2	5	70	30	30	20	150

Course Contents:

Unit No.	Topics	Teaching Hours
1	**Introduction Understand basic Encryption Concepts:** Symmetric Cipher Model, Cryptography, Cryptanalysis and Attacks; Substitution and Transposition techniques, Traditional Ciphers.	05
2	**Mathematics of Cryptography:** Integer Arithmetic, Modular Arithmetic, Matrices, Linear Congruence, Algebraic Structures, GF (2^n) Fields, Primes, Primality, Factorization, Chinese Remainder Theorem, Exponentiation and Logarithm.	05
3	**Symmetric Key Cryptography:** Stream ciphers and block ciphers, Block Cipher structure, Feistel Cipher, Diffusion and Confusion, Data Encryption standard (DES) with example, strength of DES, Design principles of block cipher, AES, Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode, RC4 algorithm, Confidentiality using Symmetric encryption, Key Distribution, Random Number Generator.	08
4	**Asymmetric Key Cryptography:** Principles, RSA, Public Key Management, Deffie Helman Key Exchange, Elliptic Curve Cryptography.	06
5	**Message Authentication and Hash Functions:** Authentication Requirements, Authentication Functions, MAC, Hash Functions, Security of Hash Functions and MACs, SHA, MD5.	05

6	**Digital Signatures and Authentication Applications:**	03
	Digital Signatures, Authentication Protocols, DSS, Kerberos, X.509, Public key Infrastructure.	
7	**Email, IP and Web Security:**	
	PGP, S/MIME, IPSec Architecture, Authentication Header, ESP, Combining Security Association, Key Management, Web Security Consideration, SSL and TLS, Introduction to ECommerce, Secure Electronic Transaction (SET).	03
8	**System Security:**	
	Intruders, Intrusion Detection, Virus and Worms, Virus Counter-Measures, DDOS attack, Firewall Design Principles, Trusted Systems.	05
9	**Cyber Security:**	
	Cyber Security Risk and Threat Management; Cyber-security Metrics in practice; Cyber Security Laws; Regulations and Ethics; Cyber Laws and Cyber Acts (IT Act 2000).	05
	TOTAL	**45**

List of Reference Books:

1. William Stallings, "*Cryptography and Network Security – Principles and Practice*", Pearson Education.
2. Bruce Scheneir, "*Applied Cryptography*", John Wiley.
3. Behrouz Forouzan, "*Cryptography & Network Security*", TMH.
4. Atul kahate, "*Cryptography and Network Security*", McGraw Hill publication
5. Menezes, Oorschot, Vanstone, "*Handbook of Applied Cryptography*", CRC Press.
6. D Stinson, "*Cryptography: Theory and Practice*", Chapman & Hall.

Course Outcomes (COs):

After learning the course students will be able to

1. Define the concepts of Information security and their use.
2. Understand basic mathematics related to Cryptography
3. Apply the various symmetric Encryption algorithms and Asymmetric Encryption Algorithms.
4. Apply the concepts of hashing with algorithms, message authentication, digital certificates, DSA and their requirement.
5. Configure Firewall for system and network security.
6. Understand basics of malware and Cyber Security.