Name of the Programme: MCA
Course Code: CSA-523
Title of Course: Cryptography and Network Security
Number of Credits: 4 (4L-0T-0P)
Effective from AY: 2022-23

Prerequisites for the course	Internet Technologies	
Objectives	1. To understand the basics of Cryptography and Network Security. 2. To be able to secure a message over an insecure channel by various means. 3. To learn about how to maintain the Confidentiality, Integrity and Availability of data. 4. To understand various protocols for network security to protect against the threats in the networks.	
Content	**Foundations of Cryptography and Security** Ciphers and Secret Messages, Security Attacks and Services. Classical encryption techniques. **Mathematical Tools for Cryptography** Substitutions and Permutations, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic. **Design Principal of Block Ciphers** Theory of Block ciphers, Feistel Cipher network Structures, DES and triple DES, Modes of Operation (ECB, CBC, OFB, CFB), Strength of DES, AES **Pseudo Random Numbers and Stream Ciphers** Pseudo random sequences, Linear Congruential generators, Cryptographic generators, Design of stream Ciphers, RC4. **Public Key Cryptography** Prime Numbers and testing for primality. Factoring large numbers, Discrete Logarithms. **Asymmetric Algorithms** RSA, Diffie-Hellman, ElGamal, Introduction of Ecliptics curve cryptosystems, Key Management, Key exchange algorithms, Public Key Cryptography Standards. **Hashes and Message Digests** Message Authentication, MD5, SHA-3, HMAC **Digital Signatures, Certificate and Standards** Digital signature standards (DSS and DSA), Public Key Infrastructures, Digital certificates and Basics of PKCS standards. **Authentication** Kerberos , X509 Authentication Service **Web Security protocols** IP Security, Transport Layer Security(TLS), Wireless Security, **System Security** Intrusion detection , Password management, Firewalls management	6 hours 3 hours 9 hours 3 hours 3 hours 9 hours 6 hours 6 hours 3 hours 6 hours 6 hours
Pedagogy	Lectures/ Hands-on assignment/tutorials/Presentations	
References/ Readings	Main Reading: 1. Stallings William, " Cryptography and Network Security: Principles and Practises", 5th edition, Prentice Hall 2. Kahate Atul, "Cryptography and Network Security" Tata McGraw-Hill.	
Course Outcomes	1. Provide security of the data over the network. 2. Implement various networking security protocols. 3. Protect any network from the threats in the world.	