**SRI RAMAKRISHNA MISSION VIDYALAYA**

**COLLEGE OF ARTS & SCIENCE- COIMBATORE - 641 020**

For candidates admitted from academic year 2013-2014 onwards under New CBCS.

BCA- **CYBER SECURITY**

**Year : Semester : v**

**Hours / Week : Subject Code : 13UCA5ELT1**

**Credits :**

**Unit I**

Foundations of Cryptography and Security :- Ciphers and Secret Message, Security Attacks and Services. Mathematical Tools for Cryptography : Substitutions and Permutations, Modular Arithmetic, Euclid’s Algorithm, Finite Fields, Polynomial Arithmetic. Design Principle of Block ciphers: Theory of Block Cipher Design. Cipher Network Structures, DES and Triple DES, Modes of Operation ( ECB, CBC, OFB, CFB) , Strength of DES

**Unit II**

Block Cipher Algorithms:- IDEA, CAST, Blowfish , Twofish , Rijndael (AES). Pseudo Random Numbers and stream ciphers: Pseudo random sequences, Linear Congruential Generators, Cryptographic Generators, Design of Stream Cipher , RC4, RC5.

**Unit III**

Public Key Cryptography:- Prime Numbers and Testing for Primality, Factoring Large Numbers, Discrete Logarithms RSA, Diffie- Hellman, ElGamal , Introduction of Elliptic acre Cryptosystems Key Management , Key Exchange Algorithms, Public – Key Cryptography Standards. Hashes and Message Digests: Message Authentication, MD5, SHA-1, RIPEMD, HMAC.

**Unit IV**

Digital Signatures, Certificates, and Standards:- Digital Signature Standard ( DSS and DSA ), Public key Infrastructure, Digital Certivicates and Basics of PKCS Standards. Authentication: Kerberos V 4 and V 5, X.509 Authentication Service. Electronic Mail Security : Pretty Good Privacy ( PGP) , S /MIME, X.400 . IP and Web Security Protocols: IPSec and Virtual Private Networks, Secure Sockets and Transport Layer ( SSL and TLS).

**Unit V**

System Security: - Computer Virus, Firewall and Design Principles, Cryptography and Network Security. Electronic Commerce Security: Electronic Payment Systems, Secure Electronic Transaction ( SET), Protocols (CyberCash, iKey) Ecash ( DigiCash ), Smart Card Based Systems.

**TEXT BOOKS:**

1. Cryptography and Network Security, William Stalling, 4th Edition, PHI.

**REFERENCE BOOKS:**

1. Applied Cryptography: Protocols & Algorithms, Schneier& Bruce, MGH