# CRYPTOGRAPHY AND NETWORK SECURITY

## MIT(CS)-204

### Block –I

**Unit I:** **(Cryptography and Network Security)** Introduction to Network Security, Classical Cryptography, Substitution Ciphers and Cryptanalysis, Transposition Ciphers and Cryptanalysis

**Unit II:** (**Number Theory**) Introduction to Number Theory, Modular Arithmetic, Modular Exponentiation, Algebraic Structures & Finite Fields I, Algebraic Structures & Finite Fields II

**Unit III:** **(Prime's Euler and Fermat's Theorem)** Introduction to Prime's Euler and Fermat's Theorem, Euler's Theorems, Fermat Primes

**Unit IV:** **(Chinese Remainder Theorem, Exponentiation and Logarithm)** Introduction to Chinese Remainder Theorem, Exponentiation and Logarithm, Finite Multiplicative Group, Cyclic groups and generators, Tabulation of Discrete Logarithms

### Block –II

**Unit V:** **(Introduction to modern Cryptography**) Introduction, Stream Cipher, Block Cipher, Digital Signature, Digital Certificate

**Unit VI:** **(RIVEST CIPHER (RC4))** Introduction to RC4, Types of RC4, Application of RC4, Simplified DES

**Unit VII:** **(Data Encryption Standard)** Introduction to Data Encryption Standard (DES), Encryption Overview, DES Round Structure, Strength of DES

**Unit VIII:** (**Modes of Operations**) Introduction to m3 Basic Modes Of Operations, Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR) , Advanced Encryption Standard, AES Key Scheduling

### Block –III

**Unit IX:** **(Public key cryptography and RSA cryptosystem)** Definition: symmetric cryptography and asymmetric cryptography, symmetric and asymmetric cryptography, Public Key Cryptography , Digital Signature and Digital Certificate, RSA public key cryptosystem and algorithm ,Security features in RSA

**Unit X:** (**Elgamal Cryptosystem And Elliptic Curve Cryptosystem**) Elgamal public key crypto system, Elgamal Encryption process, key generation process and example , Elliptic curves and cryptosystems, Compare with Elgamal Cryptosystem , security of ECC

**Unit XI:** **(Key Management and Diffie-Hellman Key Exchange)** Public-key encryption schemes, Public-key certificate schemes and security, Diffie-Hellman key management protocol, ECC and ECC- Diffie Hellman, symmetric-key agreement, man-in-middle attack

**Unit XII:** **(Security Models, Hash and Mac Algorithms)** Types of Access Control, Concept of Security Models, Trust models (Bell-LaPadula (BLP),Biba, clark-wilson), Finite State Machine Models, Hash function, algorithm and properties , Keyed Hash Function Macs (HMAC), Message Security Requirements, Public-Key Message Encryption, Message Authentication Code (Mac), Secure Hash Algorithm categories, SHA-512, cryptographic MAC function, categories of MAC function,

structure of HMAC and CMAC.

**Block –IV**

**Unit XIII:** **(Digital Signature)** Introduction to Digital signature, Digital Signature Standard, The Digital Signature Algorithm, Kerberos, Kerberos Version 4 &5, Public Key Infrastructure and certificate

**Unit XIV:** **(Electronic Mail security-PGP, Security Attack, IP Security)** Introduction to Electronic Mail security-PGP, Security Attack and types, IP Security

**Unit XV:** **(Web Security: SSL and TLS)** Web Security Considerations, Web Traffic Security Approaches, Web Security: SSL and TLS, Firewalls and components, Need of Security in Networks

**Unit XVI:** **(Introduction to Wireless LAN Security, WLAN Security**) Introduction to WLAN and Topologies, 802.11 MAC, WLAN Security