Cryptography & Network Security

MODULES	HOURS
Introduction: Classification of Possible attacks, Traditional Encryption Techniques: Affine, Play Fair, Hill cipher and Vernam cipher with subsequent strength analysis. Symmetric key & Asymmetric key cryptography, Block & Stream Cipher, Stream Cipher generation technique LFSR.	4
Symmetric Key Cryptography: Modular Arithmetic, Extended Euclidean Algorithm, Group, Ring and Finite Field, Polynomial Arithmetic, Shannon's Theorem, Feistel structure, DES and AES algorithm with strength analysis, Diffie Hellman Key Exchange Problem & Man-in-the Middle attack, 2 DES and 3 DES. Algorithmic Modes.	9
Asymmetric Key Cryptography: Fermat's and Euler's Theorem, Primality Testing, Discrete Logarithm, The Chinese Remainder Problem, RSA, Elgamal, Eliptic Curve algorithms with necessary mathematical analysis,	9
Message Integrity: Hash function, Hash function criteria, Evaluating the security of Cryptographic hash functions, MAC, Brief idea on MD5, SHA-1, H-MAC.	3
Authentication techniques: Password Based and Challenge Response based authentications, Role of KDC in Key-exchange and Authentication, Needham Schroder algorithm, Kerberos	3
Security layers in Network Protocol Stack: IP Sec, AH & ESP, Transport & Tunnel Modes, Security Association, IKE protocol, Secure Socket Layer, Security protocols used in Application layer like PGP, SHTTP etc.	6
Digital Signature: Concepts and the techniques through RSA, Basics of Steganography.	4
Network Defense tools: Firewalls, Intrusion Detection, Filtering, Security in Mobile Platforms: Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities.	2