COER UNIVERSITY
FORMERLY KNOWN AS UETR

SYLLABUS

Cryptography & Network Security

S. No.	Contents
1.	Introduction & Number Theory:Services, Mechanisms and attacks-the OSI security architecture-Network security model-ClassicalEncryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid‟s algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat‟s and Euler‟s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms.
2.	Block Ciphers & Public Key Cryptography: Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key Exchange-Elliptic curve arithmetic-Elliptic curve cryptography.
3.	Hash Function & Digital Signature: Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 – SHA – HMAC – CMAC – Digital signature and authentication protocols – DSS – EI Gamal – Schnorr.
4.	Security Practice & System Security: Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of cryptography and security.
5.	Email, IP & Web Security: E-mail Security: Security Services for E-mail-attacks possible through E-mail – establishing keys privacy-authentication of the source-Message Integrity-Non-Repudiation-Pretty Good PrivacyS/MIME. IPSecurity: Overview of IPSec – IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET)

1. Suggested Books:

S. No.	Name of Books / Authors	Year of Publication
1.	William Stallings, Cryptography and network security, Pearson Education.	2014

2.	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press.	2001
3.	Margaret Cozzens, Steven J Miller, The mathematics of encryption, American Mathematical Society.	2013