CRYPTOGRAPHY

Course Syllabus
June 2014

Prerequisites: NONE **Course Credits: 4**

UNIT - I: OVERVIEW, HISTORY AND CLASSICAL CIPHERS

Cryptography, steganography and cryptanalysis; History and development of cryptography; Classical cryptosystems: shift, substitution and Vigen´ere ciphers; Attacks on shift, substitution and Vigen´ere ciphers; Enigma cryptosystem and Role of WW-II; Designing a provably secure system, One-Time pads.

UNIT - II: SYMMETRIC KEY CRYPTOSYSTEMS AND GSM SECURITY

Basics of number theory and algebra; Introduction to information theory, Shannon's axioms; DES and AES; Encryption in GSM communications, A5 family of algorithms.

UNIT - III: ASYMMETRIC KEY CRYPTOSYSTEMS AND DIGITAL SIGNATURES

Prime numbers, factorisation and discrete logarithms; RSA and El Gamal cryptosystems; Signa-ture schemes, hash functions and secret sharing schemes.

UNIT - IV: INTRODUCTION TO CRYPTANALYSIS

Known plaintext, known ciphertext, chosen plaintext and chosen ciphertext attacks, man-in-the-middle attacks; Attacks on DES and AES, differential cryptanalysis; Attacks on RSA; Attacks on El Gamal; Attacks on A5 family.

UNIT - V: ADVANCED TOPICS

Zero knowledge proofs; Pseudo-random number generators; Industry standards and practices.

TEXTBOOKS:

Recommended:

Douglas Stinson. *Cryptography: Theory and Practice*, Third Edition or higher, Chap-man & Hall/CRC (Indian Edition) 2011.

Alfred Menezes, Paul C. van Oorschot and Scott A. Vanstone. *Handbook of Applied Cryptography*, CRC Press (2001).

Free download in PDF available from http://cacr.uwaterloo.ca/hac/

References:

Johannes Buchmann. *Introduction to Cryptography*, Springer Pubs., 2nd Edition (2004)

Lawrence C. Washington. *Elliptic Curves, Number Theory and Cryptography*, Chapman & Hall/CRC 2nd Edition (2008).

Simon Singh. *The Code Book*, 4th Estate Pubs. (2002)