Introduction to Cryptography (CSC-313)
Tribhuvan University
Institute of Science and Technology
Soch College of Information Technology

Course Title: Introduction to Cryptography
Course no: CSC-313 ---------- **Full Marks:** 60+20+20
Credit hours: 3 ---------- **Pass Marks:** 24+8+8
Nature of course: Theory (3 Hrs.) + Lab (3 Hrs.)
Goal: The course objective is to familiarize basic concepts of cryptography so as the students can use their understanding for information security purpose.

Course Contents:

Unit 1. Introduction ---------- 4 Hrs.
Security, Attacks, Attack Types, Viruses, Worms, Trojan Horses, Classical Cryptography

Unit 2. Basics of Modern Cryptography ---------- 5 Hrs.
Plaintext, Ciphertext, keys, simple ciphers, public key cryptography, digital signatures

Unit 3. Conventional Encryption / Secret Key Cryptography ---------- 10 Hrs.
Cryptography, Cryptanalysis, Cipher Structure, Encryption Algorithms, Data Enncryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Modes of Operation, Symmetric Block Ciphers, Cipher Block Chaining (CBC), Multiple Encryption DES

Unit 4. Public Key Cryptography ---------- 6 Hrs.
Basic Number Theory, Factorization, Diffie-Hellman Key Exchange, Public Key Cryptography Algorithms, RSA.

Unit 5. Digital Signatures ---------- 4 Hrs.
One-time signatures, Digital Signature Standard (DSS).

Unit 6. Hashing and Message Digests ---------- 6 Hrs.
Hashes, Motivation and applications. Cryptographically Secure Hashing, Secure Hash Algorithm (SHA), Encryption with Message Digest (MD), MD5.

Unit 7. Authentication and Public Key Infrastructure (PKI)---------- 5 Hrs.
Overview of Authentication Systems (Password, Address, Cryptographic), Security Handshake Pitfalls, Authentication Standards, Kerberos, PKI Trust Models.

Unit 8. Network Security ---------- 5 Hrs.

IP Security, Web Security, Secure Socket Layer (SSL), Transport Layer Security (TLS), Different versions of SNMPs, PGP.

Text books / Reference books :

D. R. Stinson. Cryptography: Theory and Practice. CRC Press
William Stallings, Network Security Essentials-Applications & Standards, Pearson.
Charlie Kaufman, Radia Perlman, Mike Speciner, Nework Security Private Communication in a Public World, Second Edition, 2004,Pearson.
Matt Bishop, Computer Security, Art and Science, Pearson
Bruce Schneier, Applied Cryptography, Pearson