IS353 & 353L Cryptographic Design Engineering / Laboratory			
Credit Hours	3-1-4	**Prerequisites**	IS-201

Course Learning Outcomes:

S No	CLO	Domain	Taxonomy Level	PLO
1	Understand the history of cryptography	Cognitive	2	1
2	Comprehend fundamental principles of cryptography	Cognitive	2	1
3	Analyze cryptographic techniques and algorithms	Cognitive	4	3
4	Evaluate experimentally algorithms for encrypting data, hashing and other applications	Psychomotor	5	4

Course Content:

Chronological account of cryptography including classical shift, permutation and substitution ciphers, One Time Pad (OTP) and rotor cipher machines. Basic mathematics for cryptography including group and field theory, modular arithmetic, probability and information theory. Fundamental cryptographic principles like Confidentiality, Integrity, Availability (CIA), confusion and diffusion, non-linearity, randomness and entropy. Major types of cryptographic functions including Symmetric and Asymmetric ciphers and basic structure of Block, Stream and Public Key encryption algorithms, Hash functions, Digital Signatures. Introduction to elliptic curves, cryptographic groups defined over these curves and foundations of elliptic curve cryptography.

Teaching Methodology:

Lectures, Written Assignments, Semester Project, Presentations

Course Assessment:

Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam

Reference Materials:

1. Nigel P. Smart, Cryptography: An Introduction, 3rd Edition, ISBN 0077099877, 9780077099879, 2004
2. Nigel P. Smart, Cryptography Made Simple, ISBN 978-3-319-21936-3, 2016
3. Delfs, Hans, Knebl, Helmut, Introduction to Cryptography, ISBN 978-3-642-87126-9, 2002

Additionally, there would be lecture notes and selected articles.