IS453 Cryptanalysis					
Credit Hours:	3-0-3	**Prerequisites**	IS353		
Course Learning Outcomes:					
S No	**CLO**		**Domain**	**Taxonomy Level**	**PLO**
1.	Comprehend basic algebra and probability theory applications in cryptanalysis		Cognitive	2	1
2.	Apply techniques for basic cryptanalytic attacks		Cognitive	3	3
3.	Analyze mathematical foundations of the security of ciphers and digest and explain how cryptographic primitive work		Cognitive	4	2
4.	Implement cryptanalytic attacks against variety of ciphers		Psychomotor	3	3
Course Content:					
Cryptanalysis employs mathematical and algorithmic tools to evaluate the security level of cryptographic systems and protocols. The course explains standard cryptanalysis techniques used for analyzing and attacking different types of cryptographic schemes, focusing on aspects of private and public-key cryptography. It includes an overview of the basics of cryptanalysis followed by introduction to cryptanalysis techniques of classical ciphers (mono-alphabetic, poly-alphabetic, Frequency Analysis, Kaisiski and Friedman Tests). The focus is then shifted to cryptanalysis of modern ciphers including Block ciphers (Linear & Differential Cryptanalysis, Related Key attacks), Stream ciphers (Berlekamp Massey algo, Correlation & Fast Correlation attacks), Public Key based ciphers (Discrete Log & Integer Factorization) and Elliptic Curve based ciphers.					
Teaching Methodology:					
Lectures, Written Assignments, Semester Project, Presentations					
Course Assessment:					
Midterm Exam, Home Assignments, Quizzes, Project, Presentations, Final Exam					
Reference Materials:					
1. A course in Number Theory and Cryptography 2d ed - Neal Koblitz. 2. Algebraic aspects of Cryptography - Neal Koblitz. 3. Linear and Differential Cryptanalysis - Turorial by Howard Heyes					

4. Fast Correlation Attacks. - Paper by Matsui et al.

In addition there will be lecture notes and selected articles.