Course Code	CSE793A
Course Name	Topics in Cryptanalysis
Credits	4
Course Offered to	UG/PG
Course Description	This course aims for analyzing the security of various cryptosystems. The course will befocusing mainly on the fundamentals of cryptanalysis techniques as mentioned: Differential Cryptanalyis Linear Cryptanalysis Meet in the Middle Attack Rebound Attack Time-Memory Trade-off Attack Hash function attacks (Damgaard's MD4 attack, Wang's attack on MD4, MD5, SHA-1) Attacks against RSA, Number Field Sieve Side channel attacks (Cache timing, Fault attacks, Memory remanence) Algebraic attacks Quantum Attacks (Shor's algorithm, Grover's algorithm) etc.

Pre-requisites

Pre-requisite (Mandatory)	Pre-requisite (Desirable)	Pre-requisite(other)
None	Applied Cryptography	

*Please insert more rows if required

Post Conditions*(For suggestions on verbs please refer the second sheet)

CO1	CO2	CO3	CO4
Students are able to read, interpret and write theoretical papers in Cryptography.	Students are able to learn about various attack techniques on Cryptosystems	Students are able to propose new and improved attacks on various Cryptosystems	Students are able to analyse overall security of existing cryptosystems

Weekly Lecture Plan

Week Number	Lecture Topic	COs Met	Assignment/Labs/Tutorial
Week 1	Introduction to Topics in Cryptanalysis	C01	
Week 2	DES algorithm introduction,DES Cryptanalysis (basic idea)	C01	
Week 3	DES cryptanalysis	C01	
Week 4	DES cryptanalysis	C01, C02	
Week 5	DES cryptanalysis	C01, C02	
Week 6	DES cryptanalysis	C01, C02	
Week 7	Linear Cryptnalaysis-introduction	C01	
Week 8	Linear Cryptnalaysis (tentative)	C01, C02	
Week 9	Linear Cryptnalaysis (tentative)	C01,C02	
Week 10	SSL/TLS (tentative)	C02, C03	
Week 11	SSL/TLS (tentative)	C02, C03	
Week 12 onwards	Class presentations	C03, C04	

*Please insert more rows if required

Weekly Lab Plan

Week Number	Laboratory Exercise	COs Met	Platform (Hardware/Software)

*Please insert more rows if required

Assessment Plan

Type of Evaluation	% Contribution in Grade
Mid Semester	20%
End Semester	20%
Project evaluation	50%
Attendence	10%

*Please insert more row for other type of Evaluation

Resource Material

Type	Title
Lecture notes	Class notes
Lecture Slides	