DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

COURSE PLAN – PART I			
Name of the programme and specialization	**M.Tech. CSE**		
Course Title	Principles of Cryptography		
Course Code	CS617	**No. of Credits**	**3**
Course Code of Pre-requisite subject(s)	**Nil**		
Session	**July 2018**	**Section (if, applicable)**	**NA**
Name of Faculty	**Dr. R. Leela Velusamy**	**Department**	**CSE**
Email	**leela@nitt.edu**	**Telephone No.**	**0431-2503201**
Name of Course Coordinator(s) (if, applicable)	**NA**		
E-mail	**NA**	**Telephone No.**	**na**
Course Type	**Elective course**		

Syllabus (approved in BoS)

COURSE OBJECTIVES

- To gain knowledge about the mathematics of Crptographic algorithms
- To get an insight into the working of different existing Crptographic algorithms
- To learn how to use Crptographic algorithms in security

COURSE OUTCOMES (CO)

- Ability to build a new unbreakable cryptosystem
- Ability to blend the existing cryptographic algorithms with the existing communication protocols
- Ability to analyze and apply cryptography for secure ecommerce

Course Outcomes	**Aligned Programme Outcomes (PO)**

Course Outcome (CO)	**Programme Outcomes**							
	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6	PO-7	PO-8
Ability to build a new unbreakable cryptosystem	S	M	M	S				
Ability to blend the existing cryptographic algorithms with the existing communication protocols	S	M	M	S				

Ability to analyze and apply cryptography for secure ecommerce	S	M	M	S					

COURSE PLAN – PART II

COURSE OVERVIEW

The modern study of cryptography investigates techniques for facilitating interactions between distrustful entities. In our connected society, such techniques have become indispensable enabling, for instance, automated teller machines, secure wireless networks, internet banking, satellite radio/television and more. Cryptography is only one (important) part of security. We focus on some of the fundamental design paradigms and notions that will allow one to critically evaluate cryptographic protocols.

COURSE TEACHING AND LEARNING ACTIVITIES

S.No.	Topic	Mode of Delivery	
Unit - I			
1.	Group, cyclic group, cyclic subgroup, field	Board	
2.	Probability revised	Board	
3.	Number Theory: Fermat's theorem	Board	
4.	Cauchy 's theorem and its application in Cryptography	PPT & Tutorial	
5.	Chinese remainder theorem	PPT & Tutorial	
6.	primality testing algorithms	PPT & Tutorial	
7.	Euclid's algorithm for integers, quadratic residues, Legendre symbol, Jacobi symbol	PPT & Tutorial	
UNIT - II			
1.	Cryptography and cryptanalysis,	Board	
2.	Classical Cryptographic techniques	PPT & Tutorial	
3.	different type of attack: CMA,CPA,CCA,	PPT	
4.	Shannon perfect secrecy, OTP, Pseudo random bit generators,	PPT	
5.	stream ciphers	Board	
6.	RC4	Board	
UNIT – III			
1.	Block ciphers: Modes of operation	Board	
2.	DES and its variants	PPT	
3.	AES	PPT	
4.	linear and differential cryptanalysis	Pen-Board & Tutorial	
UNIT – IV			
1.	One-way function , trapdoor one-way function	Pen-Board	
2.	Public key cryptography, Discrete Logarithm problem	Pen-Board	
3.	RSA cryptosystem	PPT & Tutorial	
4.	Diffie-Hellman key exchange algorithm	PPT & Tutorial	
5.	Elgamal Cryptosystem	PPT & Tutorial	
UNIT – V			
1.	Cryptographic hash functions, secure hash algorithm	PPT	

2.	Message authentication	PPT	
3.	Digital signature, RSA digital signature	PPT	
4.	Elgamal digital signature	PPT & Tutorial	
	Total	36	

COURSE ASSESSMENT METHODS (shall range from 4 to 6)

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Cycle Test – 1	8th Week	1 Hour	20
2	Cycle Test – 2	13th Week	1 Hour	20
3	Assignment	7th &10th Week	1 week each	10
4				
CPA	Compensation Assessment*	11th week	1 Hour	20
5				
6	Final Assessment *	Last Week of November	3 Hour	50

***mandatory; refer to guidelines on page 4**

COURSE EXIT SURVEY (mention the ways in which the feedback about the course shall be assessed)

Through MIS Feedback System

COURSE POLICY (preferred mode of correspondence with students, compensation assessment policy to be specified)

MODE OF CORRESPONDENCE (email/ phone etc): Phone
COMPENSATION ASSESSMENT POLICY   Retest for genuine case

ATTENDANCE POLICY (A uniform attendance policy as specified below shall be followed)

- **At least 75% attendance in each course is mandatory.**
- **A maximum of 10% shall be allowed under On Duty (OD) category.**
- Students with **less than 65% of attendance** shall be prevented from writing the final assessment and **shall be awarded 'V' grade.**

ACADEMIC DISHONESTY & PLAGIARISM

- Possessing a mobile phone, carrying bits of paper, talking to other students, copying from others during an assessment will be treated as punishable dishonesty.

- Zero mark to be awarded for the offenders. For copying from another student, both students get the same penalty of zero mark.

- The departmental disciplinary committee including the course faculty member, PAC chairperson and the HoD, as members shall verify the facts of the malpractice and award the punishment if the student is found guilty. The report shall be submitted to the Academic office.

The above policy against academic dishonesty shall be applicable for all the programmes.

ADDITIONAL INFORMATION

Textbooks, reference books

1. Stinson. D. Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2010.
2. W. Stallings, Cryptography and Network Security Principles and practice, 5/e, Pearson Education, Asia, 2012.
3. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security,
   second edition, Tata McGraw Hill, 2011
4. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005

FOR APPROVAL

R. Leela	R. Leela	R. Leela
Course Faculty **R. LEELA VELUSAMY**	**CC-Chairperson** **R. LEELA VELUSAMY**	**HOD** **R. LEELA VELUSAMY**