



NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE PLAN – PART I			
Name of the programme and specialization	M.Tech. CSE		
Course Title	Advanced Cryptography		
Course Code	CS611	No. of Credits	3
Course Code of Pre-requisite subject(s)	NIL	-	-
Session	July 2020	Section (if, applicable)	NIL
Name of Faculty	R. Leela Velusamy	Department	CSE
Official Email	leela@nitt.edu	Telephone No.	7598603413
Name of Course Coordinator(s) (if, applicable)	NA		
Official E-mail		Telephone No.	
Course Type (please tick appropriately)	<input type="checkbox"/> Core course	<input checked="" type="checkbox"/> Elective course	
Syllabus (approved in BoS)			
<p>UNIT-I Number Theory Review of number theory, group, ring and finite fields, quadratic residues, Legendre symbol, Jacobi symbol, Probability, Discrete random variable, Continuous random variable, Markov's inequality, Chebyshev's inequality, normal distribution, the geometric and binomial distributions.</p> <p>UNIT-II Formal Notions Of Attacks Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model.</p> <p>UNIT-III Public Key Cryptography Public key cryptography, probabilistic encryption, homomorphic encryption, Elliptic curve cryptosystems, Cryptographic hash functions.</p> <p>UNIT-IV Digital Signatures Digital signatures and the notion of existential unforgeability under chosen message attacks. Schnorr signature scheme. Zero Knowledge Proofs and Protocols,</p> <p>UNIT-V Blockchain Technology Blockchain technology, Consensus algorithm, Incentives and proof of work, Smart contract, Bitcoin.</p>			



Text Books

1. W. Mao, *Modern Cryptography: Theory & Practice*, Pearson Education, 2014.
2. *Introduction to Modern Cryptography (2nd edition)*: Jonathan Katz and Yehuda Lindell, CRC Press, 2015.
3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies*, 2016.

Reference Books

1. Koblitz, N. *Course on Number Theory and Cryptography*, Springer Verlag, 1986 4.
2. Menezes, A, et.al. *Handbook of Applied Cryptography*, CRC Press, 1996.
3. Thomas Koshy, *Elementary Number Theory with applications*, Elsevier India, 2005.

COURSE OBJECTIVES

- To study the concepts of applied cryptography
- To understand the application of cryptographic techniques in real world applications
- To comprehend the notion of provable security and its implication with improved security guarantees

MAPPING OF COs with POs

Course Outcomes	Programme Outcomes (PO) (Enter Numbers only)
1. Break cryptosystems that are not provably secure	PO1-PO7, PO9, PO11
2. Derive simple provable security proofs for cryptographic schemes	PO1-PO7, PO9, PO11
3. Design and implement cryptographic protocols	PO1-PO7, PO9, PO11

COURSE PLAN – PART II

COURSE OVERVIEW

This course enables the students to know about the principles of Cryptography techniques and its advances. This course deals with mathematical concepts required for developing cryptosystems, proving the cryptosystems ability to withstand attacks, developing cryptosystems for various security services etc.

COURSE TEACHING AND LEARNING ACTIVITIES

(Add more rows)

S.No.	Week	Topic	Mode of Delivery
1	1	Review of number theory, group, ring and finite fields, quadratic residues, Legendre symbol, Jacobi symbol	ONLINE- PPT
2	2	Probability, Discrete Random variable, Continuous random variable, Markov's inequality, Chebyshev's inequality, normal	ONLINE- PPT



		distribution, the geometric and binomial distributions	
3	3	Crypto systems using number theory concepts, Design, proof, and cryptanalysis	ONLINE- PPT
4	4	Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2)	ONLINE- PPT
5	5	Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model.	ONLINE- PPT
6	6	Mathematics involved in design of public key cryptographic techniques	ONLINE- PPT
7	7	Public key cryptography, probabilistic encryption, homomorphic encryption	ONLINE- PPT
8	8	Elliptic curve cryptosystems, Cryptographic hash functions.	ONLINE- PPT
9	9	Digital signatures and the notion of existential unforgeability under chosen message attacks	ONLINE- PPT
10	10	Schnorr signature scheme. Zero Knowledge Proofs and Protocols,	ONLINE- PPT
11	11	Cryptography for Blockchain technology	ONLINE- PPT
12	12	Consensus algorithm, Incentives and proof of work	ONLINE- PPT
13	13	Smart contract, Bitcoin.	ONLINE- PPT
COURSE ASSESSMENT METHODS (shall range from 4 to 6)			



S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Written Test - 1	October last week	1 hour	20
2	Online assignments/surprise test	Every week	offline	20
3	Written Test - 2	November 2 nd week	1 hour	20
4	Programming assignment	November last week	Online Demo	10
CPA	Compensation Assessment*	December 2 nd week	1 hour	20
6	Final Assessment *	December 3 rd week	2 hours	30

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

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

Feed back through online mode after Written test -1 and later through MIS

COURSE POLICY (including compensation assessment to be specified)

Students should not be absent for the written test 1 and 2. If the reason for absence is genuine, the student can appear for compensation assessment. The medical certificate/on duty certificate should be submitted within one week after rejoining. The portions for the compensation assessment will be the entire portions covering test 1 and 2.

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.




NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

- 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, IF ANY

FOR APPROVAL

Course Faculty  25/09/2020 CC- Chairperson  HOD 
R. LEELA VELUSAMY



Guidelines

- a) The number of assessments for any theory course shall range from 4 to 6.
- b) Every theory course shall have a final assessment on the entire syllabus with at least 30% weightage.
- c) One compensation assessment for absentees in assessments (other than final assessment) is mandatory. Only genuine cases of absence shall be considered.
- d) The passing minimum shall be as per the regulations.

B.Tech. Admitted in				P.G.
2018	2017	2016	2015	
35% or (Class average/2) whichever is greater.		(Peak/3) or (Class Average/2) whichever is lower		40%

- e) Attendance policy and the policy on academic dishonesty & plagiarism by students are uniform for all the courses.
- f) Absolute grading policy shall be incorporated if the number of students per course is less than 10.
- g) Necessary care shall be taken to ensure that the course plan is reasonable and is objective.