

**DEPARTMENT OF Computer Science and Engineering**  
**NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI**

COURSE PLAN – PART I			
Course Title	Advanced Cryptography		
Course Code	CSPE71	No. of Credits	3-0-0-3
Course Code of Pre-requisite subject(s)	CSPC35		
Session	July 2022	Section (if, applicable)	A and B
Name of Faculty	Dr. Kunwar Singh	Department	Computer Science and Engineering
Email	kunwar@nitt.edu	Telephone No.	9843692144
Name of Course Coordinator(s) (if, applicable)			
E-mail		Telephone No.	
Course Type	Elective course		
Syllabus (approved in BoS)			
2015-2016			
COURSE OBJECTIVES			
<ul style="list-style-type: none"><li>• To study the concepts of applied cryptography</li><li>• To understand the application of cryptographic techniques in Real world applications</li><li>• To comprehend the notion of provable security and its implication With improved security guarantees</li></ul>			
COURSE OUTCOMES (CO)			
Course Outcomes			Aligned Programme Outcomes (PO)
1. Ability to break cryptosystems that are not provably secure			PO1, PO5, PO6
2. Ability to derive simple provable security proofs for cryptographic schemes			PO3, PO5
3. Ability to design and implement cryptographic protocols			PO1, PO3, PO5, PO6

**COURSE PLAN – PART II****COURSE TEACHING AND LEARNING ACTIVITIES**

<b>S.No.</b>	<b>Week/Contact Hours</b>	<b>Topic</b>	<b>Mode of Delivery</b>
1	1/3	Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), RSA Cryptosystem	Online
2	2/3	RSA, Modified ElGamal Cryptosystem,	Online
3	3/3	Elliptic curve cryptosystems, Homomorphic encryption, Accumulators: RSA accumulator	Online
4	4/3	Paillier encryption scheme, Digital Signature: Schnorr Signature, DSA, Elliptical Digital Signature	Online
5	5/3	Paillier encryption scheme, Digital Signature: Schnorr Signature, DSA, Elliptical Digital Signature	Online
6	6/3	Blockchain Technology, Bitcoin, Smart Contract	Online
7	7/3	Commitment, Petersan's commitment scheme	Online
8	8/3	Zero knowledge proof	Online
9	9/3	Zero knowledge proof	Online
10	10/3	Multi party computation: Models and definitions of Secure Computation, Secret Sharing Schemes	Online
11	11/3	Oblivious Transfers (OT) and Extensions, Circuit Garbling	Online
12	12/3	BenOr-Goldwasser-Wigderson (BGW) Construction, Goldreich-Micali-Wigderson (GMW) construction	Online

13	13/3	Yao construction, BMR construction	Online
----	------	------------------------------------	--------

**COURSE ASSESSMENT METHODS (shall range from 4 to 6)**

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Assesment 1	4 <sup>th</sup> week of September	1 hour	20
2	Assesment 2	2 <sup>nd</sup> week of November	1 hour	20
3	Mini Project	3 <sup>rd</sup> week November		20
CPA	Compensation Assessment*	As per academic schedule	1 hour	20
5	Final Assessment *	As per academic schedule	2 hour 30 minutes	40

**Text Books**

1. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2014.
2. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, CRC, 2018.
3. Efficient Two-party Protocols- Techniques and Constructions by Carmit Hazay and Yehuda Lindell. Springer

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

- Feedbacks are collected before every Cycle Test and after the End semester exam in the feedback forms.
- Suggestions from the students are incorporated for making the course more understanding and interesting.
- Students, through their Class Representatives, may give their feedback at any time to the course faculty which will be duly addresses

**COURSE POLICY (preferred mode of correspondence with students, policy on attendance, compensation assessment, , academic honesty and plagiarism etc.)**

**MODE OF CORRESPONDENCE (email/ phone etc) :** email

**ATTENDANCE**

- 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 frpm writing the final

assessment and shall be awarded 'V' grade.

### **COMPENSATION ASSESSMENT**

The Students those have missed the cycle test 1 or cycle test 2 on medical or OD can appear for COMPENSATION ASSESSMENT (Retest) after showing the medical certificate or OD letter signed by competent authority. Portion for the retest will be portions of cycle test 1 and cycle test 2.


### **ACADEMIC HONESTY & 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.

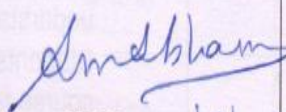
### **ADDITIONAL INFORMATION**

The students can get their doubts clarified at any time with prior appointment.

### **FOR APPROVAL**

  
Course Faculty \_\_\_\_\_

  
CC-Chairperson \_\_\_\_\_

  
HOD 22/3/2022