NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE PLAN – PART I			
Name of the programme and specialization	**B.Tech Computer Science & Engineering**		
Course Title	**Principles of Cryptography**		
Course Code	**CSPC63**		
Course Code of Pre-requisite subject(s)	**NIL**	**No. of Credits**	**3**
Session	**JANUARY 2022**	**Section (if Applicable)**	**B**
Name of Faculty	**Dr.C Mala**	**Department**	**CSE**
Official Email	**mala@nitt.edu**	**Telephone No.**	
Name of Course Coordinator(s) (if, applicable)	**NA**		
Official E-mail	**-**		
Course Type (please tick appropriately)	**PC**		

Syllabus (approved in BoS)

Refer the Link: https://www.nitt.edu/home/academics/curriculum/B.Tech-CSE-2020.pdf (Page Number 59)

COURSE OBJECTIVES

- To gain knowledge about the mathematics of the cryptographic algorithms
- To get an insight into the working of different existing cryptographic algorithms
- To learn about key exchange protocols and attacks on such protocols
- To introduce the fundamental concepts of hash functions and digital signatures
- To learn how to use cryptographic algorithms in security

MAPPING OF COs with POs

Course Outcomes	**Programme Outcomes (PO)** (Enter Numbers only)
Understand the basic concepts of symmetric cryptosystem, public key cryptosystem and digital signature scheme	
Reason about the security of cryptographic algorithms	
Evaluate the security of a protocol based on security metrics	
Justify the usage of security principles and digital signatures for any application	

COURSE PLAN – PART II			
COURSE OVERVIEW			
COURSE TEACHING AND LEARNING ACTIVITIES			**(** Add more rows)
S.No	**Week / Contact Hours**	**Topic**	**Mode of Delivery** **Online (MS Teams)**
UNIT I			
1	1	Introduction, Security Goals, Security Attacks, Security Mechanisms	√
2	2	Number Theory : Introduction	√
3	3	Fermat's Theorem	√
4	4	Cauchy's Theorem	√
5	5	Chinese remainder theorem	√
6	6	Primality Testing	√
7	7	Euclid's algorithm for integers	√
8	8	Quadratic residues	√
9	9	Legendre symbol ,Jacobi symbol	√
UNIT II			
10	10	Cryptography and cryptanalysis	√
11	11,12,13	Classical Cryptographic Techniques	√
12	14,15	Attacks: CMA, CPA, CCA	√
13	16	Shannon Perfect Secrecy	√
14	17	OTP , Pseudo random bit generators	√
15	18,19	Stream Ciphers	√
16	20	RC4	√

UNIT III			
17	21,22	Block Cipher , Modes of operation	√
18	23	Attacks on Block Ciphers	√
19	24, 25	DES	√
20	26	DES Variants	√
21	27	Security of DES	√
22	28	Finite Field	√
23	29	AES	√
24	30	Linear and Differential cryptanalysis	√
UNIT IV			
25	31	One Way Function	√
26	32	Trapdoor One-way Function	√
27	33	Public Key Cryptography	√
28	34,35	RSA Cryptosystem	√
29	36	Diffie-Hellman Key Exchange	√
30	37	ElGamal Cryptosystem	√
UNIT V			
31	39,40	Cryptographic Hash Function	√
32	41	Secure Hash Functions	√
33	42	Message Authentication	√
34	43	Digital Signature	√
35	44	RSA Digital Signature	√

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

S.No.	Mode of Assessment	Week/Date	Duration	% Weightage
1	Cycle Test – 1	6th week	1 Hour	20
2	Cycle Test – 2	12th week	1 Hour	20
3	Programming Assignment 1	7th week		10
4	Programming Assignment 2	10th Week		10
5	Programming Assignment 3	13th Week		10
CPA	Compensation Assessment*	14th week	1 Hour	20
6	Final Assessment *	As per Academic Schedule	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)

Feedbacks are collected before final examination through MIS or any other standard format followed by the institute.

COURSE POLICY (including compensation assessment to be specified**)**

MODE OF CORRESPONDENCE (email/ phone etc)

Email : mala@nitt.edu

COMPENSATION ASSESSMENT

One Retest will be conducted for absentees in Cycle Tests, for genuine reasons

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, IF ANY

The Course Coordinator is available for consultation during official timings

FOR APPROVAL

Course Faculty _____ **CC- Chairperson** _____ **HOD** _____

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.