INDIAN INSTITUTE OF TECHNOLOGY TIRUPATI

भारतीय प्रौद्योगिकी संस्थान तिरुपति

1.	Title of the course	Introduction to Modern Cryptography
2.	Course number	CS537L
3.	Status of the course	Elective
4.	Structure of credits	3-0-0-3
5.	Offered to	PG
6.	New course/modification to	New
7.	To be offered by	Department of Computer Science and Engineering
8.	To take effect from	January 2023
9.	Prerequisite	CoT
10.	Whether approved by the Department	Yes
11.	**Course Objective(s):** To introduce fundamentals of modern cryptography including definitions, proof of security and its applications. To learn various cryptographic primitives and its applications.	
12.	**Course Content:** Introduction: classical cryptography, private-key encryption, historical ciphers and their cryptanalysis; Perfectly secret encryption; Private-key cryptography: private-key encryption, message authentication, hash functions and their applications, practical constructions; Public-key cryptography: public-key encryption, Diffie-Hellman key exchange, digital signatures.	
13.	**Textbook(s):** 1. Katz J and Lindell Y, *Introduction to Modern Cryptography*, 3rd Edition, CRC Press (2021). 2. Rosulek M, *The Joy of Cryptography*, 1st Edition, Online (2021).	
14.	**Reference(s):** 1. Boneh D and Shoup V, *A Graduate Course in Applied Cryptography*, 1st Edition, Online (2020). 2. Smart N, *Cryptography: An Introduction*, 3rd Edition, Online (2013). 3. Stinson D R and Paterson M B, *Cryptography. Theory and practice*, 4th Edition, CRC Press (2019).	