भारतीय प्रौद्योगिकी संस्थान तिरुपति

TIRUPATI

INDIAN INSTITUTE OF TECHNOLOGY TIRUPATI

भारतीय प्रौद्योगिकी संस्थान तिरुपति

1.	Title of the course	Cryptography and Network Security
2.	Course number	CS501L
3.	Structure of credits	3-0-0-3
4.	Offered to	UG
5.	New course/modification to	Modification To CS5101/2
6.	To be offered by	Department of Computer Science and Engineering
7.	To take effect from	July 2022
8.	Prerequisite	CoT
9.	**Course Objective(s):** To give a clear insight into cryptography, authentication, and emerging security standards. To impart knowledge on network security protocols.	
10.	**Course Content:** Introduction to classical ciphers. Mathematical background: Shannon’s theory, computational complexity, finite fields, number theory. Concepts of pseudo-random number generator and pseudo-random functions, and their applications in designing standard ciphers such as RC4, DES, and AES. Attack models for ciphers: linear, differential, impossible differential, slide attacks. Public key cryptosystems: One way and trapdoor functions (RSA and ECC). Key exchange: The Diffie Hellman. Hash functions: SHA-1, keyed hash functions. Message authentication and signatures. Implementation aspects of ciphers and sidechannel analysis, key establishment protocols, electronic mail security, web security, and bitcoins.	
11.	**Textbook(s):** 1. Douglas R S, *Cryptography: Theory and Practice. CRC Press*, 3rd Edition, Taylor and Francis Group (2014).	
12.	**Reference(s):** 1. Alfred J M, Paul C O and Scott A V, *Handbook of Applied Cryptography*, CRC Press, Fifth printing, (1996). 2. Bruce S, *Applied Cryptography. Protocols, Algorithms, and Source Code in C.* Wiley (1996). 3. William S,Cryptography and Network Security: Principles and Practices, 6th Edition, Pearson India (2014). 4. Debdeep M and Rajat S C,Hardware Security: Design, Threats, and Safeguards, CRC Press,Taylor and Francis Group (2014).	