A 5-day workshop on
Cryptography and Cybersecurity
14 to 18 July 2025, Online Mode
Organized by IIITDM Kancheepuram, Chennai-600 127

Venue	**Online Mode**
Objective	Learn to analyze the security of in-built cryptosystems. Know the fundamental mathematical concepts related to security. Develop cryptographic algorithms for information security. Comprehend the various types of data integrity and authentication schemes.
Topics to be Covered	• **INTRODUCTION TO SECURITY**: Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security. Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis. • **SYMMETRIC CIPHERS**: Number theory – Algebraic Structures – Modular Arithmetic – Euclid's algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields • **SYMMETRIC KEY CIPHERS**: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution. • **ASYMMETRIC CRYPTOGRAPHY**: MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm • **ASYMMETRIC KEY CIPHERS**: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange –- Elliptic curve arithmetic – Elliptic curve cryptography. • **INTEGRITY AND AUTHENTICATION ALGORITHMS**: Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos • Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security
Target Audience	Faculty / Scientists / Industry Personnel / Researchers / M. Tech. / MCA / B. Tech. / BCA / and B. Sc. students working in Cryptography and Cybersecurity.
Prerequisites	Participants should have a basic working knowledge of computing, information theory and network concepts.
Registration	https://forms.gle/1XSSLJ9v3bBZMmFQA
Registration Fees	Faculty / Scientists / Industry Personnel / Researchers / M. Tech. / MCA / B. Tech. / BCA / and B. Sc. students – Rs. 1357/- (Inclusive of 18% GST & 15% Overheads on Rs. 1000/-)
Payment link	**https://www.onlinesbi.sbi/sbicollect/icollecthome.htm?corpID=634626** (Under "Payment Category", select "CCS2025")
Organizers	Organizing Chair: Dr, Amalan Joseph Antony A (Assistant Professor, CSE, IIITDM) Program Chair: Dr. Noor Mahammad SK (Associate Professor, CSE, IIITDM)