INDIANINSTITUTE OF INFORMATION TECHNOLOGY
DESIGN AND MANUFACTURING (IIITDM) KANCHEEPURAM

<table>
<tr><td>Course Code</td><td></td><td>Course Title</td><td colspan="4">Modern Cryptography</td></tr>
<tr><td rowspan="2">Dept./Faculty proposing the course</td><td rowspan="2">CSE / Dr Amalan Joseph Antony A</td><td rowspan="2">Structure (LTPC)</td><td>L</td><td>T</td><td>P</td><td>C</td></tr>
<tr><td>3</td><td>1</td><td>0</td><td>4</td></tr>
<tr><td rowspan="2">To be offered for</td><td rowspan="2">UG/PG</td><td>Type</td><td colspan="2">Core ☐</td><td colspan="2">Elective ▬</td></tr>
<tr><td>Status</td><td colspan="2">New ▬</td><td colspan="2">Modification ☐</td></tr>
<tr><td>Pre-requisite</td><td></td><td colspan="2">Submitted for approval</td><td colspan="3">Senate # 63</td></tr>
<tr><td>Learning Objectives</td><td colspan="6">• To learn the mathematical principles fundamental to cryptography.
• To understand the application of cryptographic techniques in real world applications.
• To understand the notion of provable security and its implications.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="6">• Design and implement provable secure cryptographic protocols.
• Evaluate the security of a protocol based on security metrics.
• Break a cryptosystem that is not secure.</td></tr>
<tr><td>Contents of the course (With approximate break-up of hours for L/T/P)</td><td colspan="6">Number Theory - Review of number theory, groups, rings and finite fields, quadratic residues. (6L+2T).

Introduction to Cryptography - Kerckhoff’s principle, Shannon’s perfect secrecy, classical cryptography, attack models: Ciphertext-only attack, Known-plaintext attack, Chosen-plaintext attack and Chosen-ciphertext attack. (7L+2T).

Symmetric Key Cryptography - Proof by reduction, computational hardness assumption, security notions, Chosen Plaintext Attack (INDCPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), attacks under message non-malleability: NM-CPA and NM-CCA2, inter-relations among the attack models. (8L+3T).

Public Key Cryptography - RSA cryptosystem, probabilistic encryption, homomorphic encryption, Elliptic curve cryptosystems, digital signatures and the notion of existential unforgeability under chosen message attacks, ElGamal digital signature scheme, Schnorr signature scheme, blind signature. (7L+2T)

Modern cryptographic techniques - Secret sharing, Zero Knowledge Proof, Sigma protocols, zk-SNARK, Multi-Party Computation, adversarial models, circuit garbling, oblivious transfer. (8L+3T).

Post-Quantum Cryptography - Lattice-based cryptography, learning with errors, code-based cryptography, multivariate cryptography. (6L+2T).</td></tr>
<tr><td>Text Books</td><td colspan="6">1. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, 3rd edition, CRC Press, ISBN: 978-0815354369, 2020.</td></tr>
<tr><td>Reference Books</td><td colspan="6">1. William Stallings, Cryptography and Network Security Principles and Practice, 8th Edition, Pearson Education, 2023, ISBN:978-9357059718.
2. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, ISBN: 978-8131702123, 2004.</td></tr>
</table>