Department of Computer Science and Engineering

NITK, Surathkal

CS800 – Number Theory and Cryptography

(Syllabus and Assessment Plan)

Semester: Ist M. Tech (ISE) **Academic Year:** 2018-19 **Credits:** (3-0-2) 4

A. Syllabus

(Total No. of Theory Hrs. – 32)

Sl. No.	Topic	Details	No. of Hrs.
1	Basic Concepts in Number Theory	• Divisibility • Greatest common divisors • Euclidean Algorithm • Factorization of integers • Congruence • Modular arithmetic • Quadratic residues • Quadratic reciprocity • Finite fields • Time estimates for doing arithmetic	8
2	Classical Encryption Techniques	• Symmetric Cipher Model • Substitution Techniques • Transposition Techniques	3
3	Block Ciphers	• Traditional Block Cipher Structures • The Data Encryption Standard • Advanced Encryption Standard • Block Cipher Operation	4

4	Stream Ciphers	• Stream ciphers • RC4	2
5	Pseudo Random Number Generators	• Principles of Pseudo random number generation. • Pseudo random number generators. • Randomness and Pseudo randomness.	2
6	Public Key Cryptography	• Principles of Public-Key Cryptosystems. • The RSA Algorithm. • Diffie-Hellman Key Exchange. • Elliptic curve cryptosystem. • Probabilistic encryption.	4
7	Cryptographic Hash Function	• Applications of Cryptographic hash Functions. • Hash Functions. • Message Authentication Codes. • Message Digest. • Digital Signatures	5
8	User Authentication	• Remote user-authentication principles. • Remote user-authentication using symmetric encryption.	2
9	Zero-knowledge protocol	• Overview of zero-knowledge concepts	1
10	Formal Verification	• Formal verification of cryptographic protocols: Survey. (Research paper by C.A. Meadows) • Analyzing encryption protocols using formal verification techniques. (Research paper by R.A. Kemmerer)	1

Text Books:

- Neal Koblitz, "Course on Number Theory and Cryptography", Springer-Verlag, 1986.
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- Ivan Niven, Herbert S. Zukerman, Hugh L. Montgomery, "An Introduction to the Theory of Numbers", John Wiley, 5th Edition. 2015.
- William Stallings, "Cryptography and Network Security", Pearson, 6th Edition, 2015.

B. Assessment Plan

(Theory : Laboratory :: 75 : 25)

Theory (75%)	**Laboratory (25%)**
1. Class Test: 10 %	Mid-Sem: 5%
2. Mid-Sem: 20%	End-Sem: 10%
3. End-Sem: 45	Lab Progress: 10%

Course Instructor	Secretary	Chairman
(B. R. Chandavarkar)	(DPGC)	(DPGC)