SOS: CRYPTOGRAPHY (PoA)

- Kavin Arvind(22B1019)

Week 1- 22/06 – 28/06 - Introduction: IntroModernCrypto Chapter 1, IntroMathCrypto Chapter 1

Week 2- 29/06 – 04/07 - Symmetric Cryptography: CryptoTextbook Chapters 2, 3

Week 2- 05/07 – 11/07 - Symmetric Cryptography: CryptoTextbook Chapters 5, Key Exchange and Asymmetric Cryptography: IntroMathCrypto Chapters 2.1-2.6, 3.1-3.3

Week 3- 12/07 – 18/07 – END SEM EXAMS

Week 4- 19/07 – 25/07 - Digital Signatures: IntroMathCrypto Chapter 4, Hash Functions: SeriousCrypto Chapter 6, Message Authentication Codes: SeriousCrypto Chapter 7

Week 5- 26/07 – 02/08 - Introduction to Lattice-Based Cryptography: IntroMathCrypto Chapters 7.1-7.8, NTRU Public Key Cryptosystem: IntroMathCrypto Chapters 2.10, 7.9-7.11, Lattice-Based Digital Signature Schemes: IntroMathCrypto Chapter 7.12, Introduction to Elliptic Curve Cryptography: IntroMathCrypto Chapters 6.1-6.5

Week 6- 03/08 – 09/08 – Cryptanalysis of DLP: IntroMathCrypto Chapters 2.7-2.9, Cryptanalysis of RSA: IntroMathCrypto Chapters 3.4-3.8, Pollard's Rho Method: IntroMathCrypto Chapters 5.4.-5.5, Lenstra's Factorisation Method: IntroMathCrypto Chapter 6.6, Lattice-Based Attacks: IntroMathCrypto 7.13-7.14, Perfect Secrecy: IntroModernCrypto Chapter 2

Week 7- 10/08 – 18/08 – Private-Key Security and Pseudorandomness: IntroModernCrypto Chapter 3, MACs and CRHFs: IntroModernCrypto Chapter 4, Theoretical Construction of Pseudorandom Objects: IntroModernCrypto Chapter 6

Week 8- 19/08 – 25/08 – topics if in case couldn't be completed in respective weeks. Project documentation and report writing.