1 Lecture Plan

- Discuss course content, prerequisites, grading scheme, attendance policy.

2 Course Webpage

`https://www.ee.iitb.ac.in/~sarva/courses/EE720/Spring2019.html`

3 Syllabus

	Secrecy	Integrity
Private-Key Setting	Private-Key Encryption	MACs
Public-Key Setting	Public-Key Encryption	Digital Signatures

- Perfectly Secret Encryption

- Private-Key Encryption

- Message Authentication Codes

- Practical Stream and Block Ciphers

- Number Theory, Groups, Finite Fields

- Public-Key Encryption

- Hash Functions

- Digital Signatures

4 Reference Books

- *Introduction to Modern Cryptography*, Jonathan Katz and Yehuda Lindell, CRC Press, 2015 (2nd Edition)

- *A Computational Introduction to Number Theory and Algebra*, Victor Shoup, 2008 (2nd edition). Available at `https://www.shoup.net/ntb/`

5 Prerequisites

- Asymptotic Notation (See Appendix A.2 of Katz/Lindell)

- Basic Probability (See Appendix A.3 of Katz/Lindell)

- Python programming

6 Grading Scheme

- 5% Attendance, 10% Assignments, 20% Quizzes, 25% Midsem, 40% Endsem

- Relative grading

- For AU, final score should be at CC level or above