EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 1 — January 13, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

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

2 Course Webpage

`https://www.ee.iitb.ac.in/~sarva/courses/EE720/Spring2020.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
- Exams will be closed notes with no cribsheets allowed
- Exams will be held in a different room in a Wednesday evening slot or on Saturday mornings
- Attendance will be taken 15 times. You get 0.5 marks per attended lecture with maximum attendance score capped at 5 marks.
- Relative grading
- For AU, final score should be at CC level or above

7 Announcement

- No lecture on 16th January, Thursday as I am out of town attending a workshop.
- I will make it up in an extra lecture slot. Tentative slot is January 22nd, Wednesday, 5:30pm to 7pm. Room will be announced.