EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 1 — January 5, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Discuss course content, prerequisites, grading scheme, attendance policy.
- Describe the difference between modern and classical cryptography
- Describe the syntax of private-key encryption

2 Course Webpage

`https://www.ee.iitb.ac.in/~sarva/courses/EE720/Spring2018.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 Course in Number Theory and Cryptography*, Neal Koblitz, Springer, 1994 (2nd Edition)

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

- 10% Assignments, 20% Quizzes, 25% Midsem, 45% Endsem
- Relative grading
- For AU, final score should be at CC level or above
- 80% attendance required

7 Cryptography

- The dictionary definition of cryptography is "the art of writing or solving codes".
- Modern definition: The study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.
- Modern approach to cryptography
  - Formal definitions
  - Precise assumptions
  - Proofs of security
- Private-key encryption setting
- Syntax of encryption: Message space $\mathcal{M}$, Key generation procedure $\texttt{Gen}$, Encryption procedure $\texttt{Enc}$, Decryption procedure $\texttt{Dec}$
  - $\texttt{Gen}$ is a probabilistic algorithm which generate key k
  - $\texttt{Enc}$ takes k and m and gives ciphertext c (probabilistic algorithm)
  - $\texttt{Dec}$ takes c and k and gives m
- Kerckhoffs' principle: Security relies solely on secrecy of key
  - Easier to keep a short key secret than to keep an algorithm secret
  - Easier to change key than encryption scheme
  - Standardization is easier