# CSE 590: Modern Cryptography (Spring 2019)

**Instructor:** Omkant Pandey (Office hours: Tu-Th 5:30p - 6:30p in 345 NCS)

**TA:** TBA

**Time:** Tuesdays & Thursdays, 4:00p - 5:20p

**Location:** (Old) CS 2129

**Contact:** omkant [at] cs.stonybrook.edu

**Important**: When sending me an email about the course, make sure your title starts with "[CSE 590]" (without the quotes). Mislabeled or unlabeled emails will, most likely, not be read.

## Announcements

All announcements will be made through BlackBoard.

## Course Description

In this class, we will introduce some topics in modern cryptography. The course is theoretical in nature, with emphasis on proofs and algorithmic reductions (even when discussing applied topics). No prior background in cryptography is assumed. However, students should have some mathematical maturity and be comfortable working with definitions and proofs. Some of the topics we will cover include: one-way functions, pseudo-randomness, symmetric encryption, hash functions, message integrity, digital signatures, and public-key encryption. Time permitting, we may also dive into zero-knowledge proofs and secure multiparty computation.

## Grading Policy

- Three takehome assignments
- One short presentation (in class)

## Text Book

The prescribed textbook for this course is Katz and Lindell's text Introduction to Modern Cryptography (some copies available in the library). See course webpage for previous offerings of this course for several free and excellent educational material on cryptography.

## Lecture Schedule (Tentative)

| Date | Topic | KL Chapter |
|---|---|---|
| **1/29/2019** | Introduction | Ch. 1 |
| **1/31/2019** | Shannon, Perfect Secrecy | Ch. 2 |
| **2/05/2019** | Indistinguishable Security | §3.1, §3.2 |
| **2/07/2019** | Encryption via PRGs | §3.3 |
| **2/12/2019** | CPA-Security via PRFs | §3.4,§3.5 |
| **2/14/2019** | Finish CPA-Security | §3.5 |
| **2/19/2019** | First Assignment Due, Discuss Solutions | |
| **2/21/2019** | Modes of Encryption | §3.6 |
| **2/26/2019** | Message Authentication Codes | Ch. 4 |
| **2/28/2019** | Hash Functions | Ch. 5 |
| **3/05/2019** | One-Way Functions - I | §7.1 |
| **3/07/2019** | One-Way Functions - II | §?? |
| **3/12/2019** | Hard Core Predicates | §7.3, §7.4 |
| **3/14/2019** | PRF/PRP from PRGs | §7.5, §7.6 |
| **3/19/2019** | --Spring Recess-- | |

| | | |
|---|---|---|
| **3/21/2019** | --Spring Recess-- | |
| **3/26/2019** | Second Assignment Due, Discuss Solutions | |
| **3/28/2019** | Number Theory Background | §8.1, §8.3.1 |
| **4/02/2019** | Hardness Assumptions | §8.2--§8.4 |
| **4/04/2019** | Key Management, Public-Key Revolution | Ch. 10 |
| **4/09/2019** | Public-Key Encryption - I | §11.1--§11.4 |
| **4/11/2019** | Public-Key Encryption - II | §11.4, §11.5 |
| **4/16/2019** | Digital Signatures - I | §12.1--§12.4 |
| **4/18/2019** | Digital Signatures - II | §12.5--§12.7 |
| **4/23/2019** | Trapdoors, Secret Sharing | §13.1—§13.3 |
| **4/25/2019** | Final Assignment Due, Discuss Solutions | |
| **4/30/2019** | Student Presentations | --- |
| **5/02/2019** | Student Presentations | --- |
| **5/07/2019** | Student Presentations | --- |
| **5/09/2019** | Student Presentations | --- |
| **5/??/2019** | Student Presentations | --- |

# Misc

**Note:** If you have a physical, psychological, medical or learning disability that may impact on your ability to carry out assigned course work, please contact the staff in the Disabled Student Services office (DSS), Room 133, Humanities, 632-6748v/TDD. DSS will review your concerns and determine with you what accommodations are necessary and appropriate. All information and documentation of disability are confidential.

**Note:** Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. **Any suspected instance of academic dishonesty will be reported to the Academic Judiciary**. For more comprehensive information on academic integrity, including categories of academic dishonesty, please refer to the academic judiciary website at http://www.stonybrook.edu/uaa/academicjudiciary/.