

# CS 346 - Cryptography (Spring 2015)

The objective of this course is to familiarize the students with cryptography and its applications. Topics will include historical cryptography, encryption, authentication, public key cryptography, number theory.

## Course Overview

This class will focus on understanding the **theoretical** underpinnings of cryptography. Key components of this course are understanding how to precisely formulate security definitions and how to rigourously prove theorems. This course is designed to be a **challenging theory course**. A good background and comfort in classes such as CS331 is important. A large component will be problems sets. These sets are meant to develop problem solving skills.

## Syllabus

[Syllabus](#)

## Logistics

Class Timing: Monday Wednesday 11:00 - 12:30

Class Location: GDC 1.304

[Brent Waters](#)

## Professor

Email: [bwaters@cs.utexas.edu](mailto:bwaters@cs.utexas.edu)

Office: GDC 6.810

Office Hours: Monday after class

Rishab Goyal

Email: [goyal@utexas.edu](mailto:goyal@utexas.edu)

Office (for office hours): GDC 1.302, Desk

TBA

Office Hours: Tuesday 12:30-2.

Venkata Koppula

Email: [kvenkata@cs.utexas.edu](mailto:kvenkata@cs.utexas.edu)

Office (for office hours): GDC 1.302, Desk

TBA

Office Hours: Wednesday 2-3:30.

## TAs

Andrew Poelstra

Email: [apoelstra@math.utexas.edu](mailto:apoelstra@math.utexas.edu)

Office (for office hours): GDC 1.302, Desk

TBA

Office Hours: Thursday 11-12:30.

Please try to first see if questions can be resolved with email to the TAs.

**Grading Policy**

Problem sets - 45%

In class examinations - 45%

Class participation - 5%

Research investigation 5%

Problem set solutions must be written up in Latex. Here is a [guide](#) for doing so.

**Course Information and Links**

A set of [course notes](#) were taken by in 2010 and 2012. The material and the way it is presented has naturally evolved over time, however, much of it is similar and these can serve as a supplement to a student's own notes.

Number theory handout (from Dan Boneh)  
[\(1\)](#) [\(2\)](#)

**Piazza and Canvas**

We will use piazza for class discussions. The Piazza page is [here](#).