# CS101abc Introduction to Theoretical Cryptography

**Term**: Spring 2016

**Lectures**: MW 10:30-12, 213 Annenberg

**Instructor**: Thomas Vidick

**Course website**: cms.caltech.edu/~vidick/cs101.html

## Course description

Cryptography is the art, or science, of secret writing. This course will introduce you to the definition, construction and analysis of the **major building blocks of modern cryptography**: one-way functions, pseudo-random generators, public and private-key encryption schemes, digital signature schemes, message authentication codes, and others. Time permitting we will consider some recent topics of interest such as homomorphic encryption, indistinguishability obfuscation, lattice-based cryptography and quantum-proof schemes.

## Prerequisites

A major focus of the course will be on definitions and proofs of security. As such, the most important prerequisite is **mathematical maturity**. Students are expected to be comfortable reading and writing mathematical proofs, be at ease with algorithmic concepts, and have elementary knowledge of discrete math, number theory (modular arithmetic), and discrete probability.

No programming will be required for the course.

## Textbook

The recommended textbook for this course is Katz and Lindell's "*Introduction to Modern Cryptography*" (2nd ed).