# Cryptography I - Dan Boneh

Welcome to Cryptography I! You’re joining thousands of learners currently enrolled in the course. I'm excited to have you in the class and look forward to your contributions to the learning community.

To begin, I recommend taking a few minutes to explore the course site. Review the material we’ll cover each week, and preview the assignments you’ll need to complete to pass the course. Click Discussions to see forums where you can discuss the course material with fellow students taking the class.

If you have questions about course content, please post them in the forums to get help from others in the course community. For technical problems with the Coursera platform, visit the Learner Help Center.

Good luck as you get started, and I hope you enjoy the course!

# Week 1 Course overview and stream ciphers

Week 1. This week's topic is an overview of what cryptography is about as well as our first example ciphers. You will learn about pseudo-randomness and how to use it for encryption. We will also look at a few basic definitions of secure encryption.

## 学习目标

Learn how stream ciphers work and how to use them correctly.

## Section 1: what is cryptography about?

阅读材料: Lecture slides for all six weeks 10 min

阅读材料: Course overview and additional reading resources 10 min

视频Course Overview 10 min

视频What is Cryptography? 15 min

视频History of Cryptography 18 min

## Section 2: crash course in discrete probability

视频Discrete Probability (Crash Course) 18 min

视频Discrete Probability (Crash Course, Cont.) 13 min

## Stream Ciphers 1: the one-time pad and stream ciphers

视频Information Theoretic Security and The One Time Pad 18 min

视频Stream Ciphers and Pseudo Random Generators 19 min

## Stream Ciphers 2: attacks and common mistakes

视频Attacks on Stream Ciphers and The One Time Pad 23 min

## Stream Ciphers 3: real-world examples

视频Real-World Stream Ciphers 19 min

## Stream Ciphers 4: what is a secure cipher?

视频PRG Security Definitions 24 min

视频Semantic Security 15 min

视频Stream Ciphers are Semantically Secure [optional] 10 min

## Week 1 Review Questions and Programming Project

测验: Week 1 - Problem Set 10 个问题

练习测验: Week 1 - Programming Assignment [optional] 1 个问题

# Week 2 Block Ciphers

Week 2. We introduce a new primitive called a block cipher that will let us build more powerful forms of encryption. We will look at a few classic block-cipher constructions (AES and 3DES) and see how to use them for encryption. Block ciphers are the work horse of cryptography and have many applications. Next week we will see how to use block ciphers to provide data integrity. The optional programming assignment this week asks students to build an encryption/decryption system using AES.

## 学习目标

Learn about block ciphers such as AES and how to use them to encrypt data

## Block Ciphers 1: overview

视频What are Block Ciphers? 16 min

## Block Ciphers 2: The Data Encryption Standard

视频The Data Encryption Standard 21 min

视频Exhaustive Search Attacks 19 min

视频More Attacks on Block Ciphers 16 min

## Block Ciphers 3: AES and other constructions

视频The AES Block Cipher 13 min

视频Block Ciphers From PRGs 11 min

## How to Use Block Ciphers 1: one-time key

视频Review: PRPs and PRFs 11 min

视频Modes of Operation: One Time Key 7 min

## How to Use Block Ciphers 2: many-time key

视频Security for Many-Time Key (CPA security) 22 min

视频Modes of Operation: Many Time Key (CBC) 16 min

视频Modes of Operation: Many Time Key (CTR) 9 min

## Week 2 Review Questions and Programming Project

测验: Week 2 - Problem Set 9 个问题

练习测验: Week 2 - Programming Assignment [optional] 4 个问题

# Week 3 Message Integrity

Week 3. This week's topic is data integrity. We will discuss a number of classic constructions for MAC systems that are used to ensure data integrity. For now we only discuss how to prevent modification of non-secret data. Next week we will come back to encryption and show how to provide both confidentiality and integrity. This week's programming project shows how to authenticate large video files. Even if you don't do the project, please read the project description --- it teaches an important concept called a hash chain.

## 学习目标

Learn how to ensure data integrity using Message Authentication Codes (MACs)

Learn what cryptographic hash functions are and how to use them.

## Message Integrity 1: definitions

视频Message Authentication Codes 15 min

视频MACs Based On PRFs 9 min

## Message Integrity 2: constructions

视频CBC-MAC and NMAC 19 min

视频MAC Padding 8 min

## Message Integrity 3: more constructions

视频PMAC and the Carter-Wegman MAC 15 min

## Collision Resistance 1: what is a collision resistant function?

视频Introduction 10 min

视频Generic Birthday Attack 14 min

## Collision Resistance 2: constructions

视频The Merkle-Damgard Paradigm 11 min

视频Constructing Compression Functions 8 min

HMAC: a MAC from a hash function

视频HMAC 7 min

视频Timing attacks on MAC verification 8 min

## Week 3 Review Questions and Programming Project

测验: Week 3 - Problem Set 10 个问题

练习测验: Week 3 - Programming Assignment [optional] 1 个问题

# Week 4 Authenticated Encryption

Week 4. This week's topic is authenticated encryption: encryption methods that ensure both confidentiality and integrity. We will also discuss a few odds and ends such as how to search on encrypted data. This is our last week studying symmetric encryption. Next week we start with key management and public-key cryptography. As usual there is also an extra credit programming project. This week's project involves a bit of networking to experiment with a chosen ciphertext attack on a toy web site.

## 学习目标

Learn how to use authenticated encryption and understand why it is such an important concept.

## Authenticated Encryption 1: why is it so important?

视频Active Attacks on CPA-Secure Encryption 12 min

视频Definitions 5 min

视频Chosen Ciphertext Attacks 12 min

## Authenticated Encryption 2: standard constructions

视频Constructions From Ciphers and MACs 20 min

## 2Authenticated Encryption 3: pitfalls

视频Case Study: TLS 1.2 17 min

视频CBC Padding Attacks 14 min

视频Attacking Non-Atomic Decryption 9 min

## Odds and Ends 1: how to derive keys

视频Key Derivation 13 min

## Odds and Ends 2: searching on encrypted data

视频Deterministic Encryption 14 min

视频Deterministic Encryption: SIV and Wide PRP 20 min

## Odds and Ends 3: disk encryption and creditcard encryption

视频Tweakable Encryption 14 min

视频Format Preserving Encryption 12 min

## Week 4 Review Questions and Programming Project

测验: Week 4 - Problem Set 10 个问题

练习测验: Week 4 - Programming Project [Optional]

1 个问题

# Week 5 Basic Key Exchange

Week 5. This week's topic is basic key exchange: how to setup a secret key between two parties. For now we only consider protocols secure against eavesdropping. This question motivates the main concepts of public key cryptography, but before we build public-key systems we need to take a brief detour and cover a few basic concepts from computational number theory. We will start with algorithms dating back to antiquity (Euclid) and work our way up to Fermat, Euler, and Legendre. We will also mention in passing a few useful concepts from 20th century math. Next week we will put our hard work from this week to good use and construct several public key encryption systems.

## 学习目标

Learn the basics of key exchange protocols and how they rely on simple algebra.

## Basic Key Exchange 1: problem statement

视频Trusted 3rd Parties 11 min

视频Merkle Puzzles 11 min

## Basic Key Exchange 2: two solutions

视频The Diffie-Hellman Protocol 19 min

视频Public-Key Encryption 10 min

## Number Theory 1: modular arithmetic

视频Notation 14 min

视频Fermat and Euler 18 min

视频Modular e'th Roots 17 min

阅读材料: More background on number theory 10 min

## Number Theory 2: easy and hard problems

视频Arithmetic algorithms 12 min

视频Intractable Problems 18 min

## Week 5 Review Questions and Programming Project

测验: Week 5 - Problem Set 15 个问题

练习测验: Week 5 - Programming Assignment [optional] 1 个问题

# Week 6 Public-Key Encryption

Week 6. This week's topic is public key encryption: how to encrypt using a public key and decrypt using a secret key. Public key encryption is used for key management in encrypted file systems, in encrypted messaging systems, and for many other tasks. The videos cover two families of public key encryption systems: one based on trapdoor functions (RSA in particular) and the other based on the Diffie-Hellman protocol. We construct systems that are secure against tampering, also known as chosen ciphertext security (CCA security). There has been a ton of research on CCA security over the past decade and given the allotted time we can only summarize the main results from the last few years. The lectures contain suggestions for further readings for those interested in learning more about CCA secure public-key systems. The problem set this week involves a bit more math than usual, but should expand your understanding of public-key encryption. Please don't be shy about posting questions in the forum. This is the last week of this Crypto I course. I hope everyone learned a lot and enjoyed the material. Crypto is a beautiful topic with lots of open problems and room for further research. I look forward to seeing you in Crypto II where we will cover additional core topics and a few more advanced topics.

## 学习目标

Learn how to use public key encryption works and how to use it.

## Public Key Encryption from Trapdoor Permutations

视频Definitions and Security 15 min

视频Constructions 10 min

## Public Key Encryption from Trapdoor Permutations: RSA

视频The RSA Trapdoor Permutation 17 min

视频PKCS 1 21 min

## Public Key Encryption from Trapdoor Permutations: attacks

视频Is RSA a One-Way Function? 16 min

视频RSA in Practice 13 min

## Public Key Encryption From Diffie-Hellman: ElGamal

视频The ElGamal Public-key System 19 min

视频ElGamal Security 13 min

视频ElGamal Variants With Better Security 10 min

## Public Key Encryption: summary

视频A Unifying Theme 11 min

视频Farewell (For Now) 5 min

## Week 6 Review Questions and Programming Project

测验: Week 6 - Problem Set 11 个问题

练习测验: Week 6 - Programming Assignment [optional] 4 个问题

# Week 7 Final exam

Congratulations! We are at the end of the course. This module contains only the final exam which covers the entire course. I hope everyone learned a lot during these 6 weeks. Good luck on the final exam and I look forward to seeing you at a future course!

## 学习目标

Final exam encompassing everything you learned in the course.

## Final exam covering the entire course

测验: Final Exam 13 个问题