

## **Instructor**

[Nelly Fazio](#)

## **Course Rationale**

Cryptographic techniques are an essential ingredient in the security mechanisms that protect the privacy of e-commerce transactions and the secrecy of cloud storage. This course introduces the fundamental notions underlying the design and evaluation of cryptographic primitives that are the core of the security protocols that enable our modern way of life.

## **Course Description**

This introductory, graduate-level course covers the theoretical foundations of modern cryptography. Emphasis will be placed on precise definitions, rigorous proof techniques, and analysis of the relations among the various cryptographic primitives (such as one-way functions, pseudo-random generators, pseudo-random permutations, and trapdoor permutations).

List of topics includes: computational security, cryptographic hash functions, private-key encryption, message authentication codes, public-key encryption, digital signatures, commitment schemes.

## **Pre-Requisites**

No prior knowledge of cryptography is required. However, general ease with algorithms and elementary probability theory, and maturity with mathematical proofs will be assumed.

## **Learning Objectives**

- Discuss how cryptography helps to achieve common security goals (data secrecy, message integrity, non-repudiation) and tasks (authentication).
- Explain the notions of symmetric encryption, hash functions, and message authentication, and sketch their formal security definitions.
- Describe the specifics of some of the prominent techniques for encryption, hashing, and message authentication (e.g., DES, AES, SHA-1, HMAC).
- Explain the notions of public-key encryption and digital signatures, and sketch their formal security definitions.
- Describe and implement the specifics of some of the prominent techniques for public-key cryptosystems and digital signature schemes (e.g., Rabin, RSA, ElGamal, DSA, Schnorr, OAEP, PSS/PSS-R).

- Illustrate the difference between symmetric and public-key cryptography.
- Evaluate cryptographic primitives and their implementations for correctness, efficiency, and security.

## Course Textbook

[Introduction to Modern Cryptography \[cs.umd.edu\]](http://cs.umd.edu) by Jonathan Katz and Yehuda Lindell. (2nd edition)

## Course Topics

1. Introduction
  - Classical vs. modern cryptography.
  - Information-theoretic security: Shannon's definition of perfect secrecy. Vernam's one-time pad.
  - Limitation of the information theoretic approach.
4. Computational Hardness and One-Wayness
  - One-way functions. One-way permutations. Trapdoor permutations. Concrete examples: integer multiplication and modular exponentiation.
  - Hardcore predicates. Goldreich-Levin construction.
  - Pseudo-random generators. Blum-Micali construction. Efficient instantiation: Blum-Blum-Shub construction.
  - Pseudo-random functions. Goldreich-Goldwasser-Micali construction.
  - Pseudo-random permutations. Luby-Rackoff construction.
  - $\epsilon$ -universal, universal one-way, and collision resistant hash functions. Merkle-Damgaard construction.
  - The hash-then-MAC paradigm.
8. Computationally Secure Symmetric Cryptography
  - Denition of secure symmetric encryption: IND, CPA, CCA.
  - Block-ciphers and mode of operations.
  - Message authentication codes.
  - Hash-then-authenticate paradigm.
5. Managing Shared Keys
  - The key distribution problem
  - Diffie-Hellman Key Exchange
3. Computationally Secure Asymmetric Cryptography
  - Definition of secure asymmetric encryption: IND, CPA, CCA.
  - Efficient constructions (ElGamal, RSA and Rabin's schemes) and padding schemes (OAEP+).
  - Blum-Goldwasser construction. Goldwasser-Micali construction.
4. Digital Signatures
  - Definition of secure digital signatures.

- Lamport's one-time signature scheme.
  - The hash-then-sign paradigm.
  - Rabin and RSA signature schemes. Padding Schemes (PSS, PSSR).
  - Schnorr signature scheme.
  - Signature schemes for multiple messages: chain-based and tree-based constructions.
7. A taste of more advanced topics (identification schemes, commitment schemes, secret sharing).

## **Assessment**

Grade will be based on:

- Class participation: 10%
- Assignments: 40%
- Term project (presentation and report): 50%