CSc 85030 Modern Cryptography—Spring 2015

Instructor: Assistant Professor Nelly Fazio

http://www-cs.ccny.cuny.edu/~fazio/

1 Instructor's Biography

Nelly Fazio is an Assistant Professor in the Computer Science Departments at the City College and the Graduate Center of CUNY. Her fields of interest include Cryptography and Information Security, with a focus on foundations (public-key and non-commutative cryptography) and applications (content protection, access control, and security in military scenarios). Her research is funded in part by the National Science Foundation, by the U.S. Army Research Laboratory and the U.K. Ministry of Defence, and by several CUNY research grants.

Dr. Fazio's awards include a 2013 NSF CAREER award, an NYU Sandra Bleistein Prize for "notable achievement by a woman in Applied Mathematics or Computer Science", an EU Marie Curie Fellowship, and an honorable mention for the NYU Janet Fabri Prize for an "outstanding dissertation in Computer Science".

Dr. Fazio received her Ph.D. from New York University, under the supervision of Prof. Yevgeniy Dodis. Her doctoral training also included research visits at Stanford University, at the Ecole Normale Superieure in Paris, France, and at Aarhus Universitet, Denmark. Before joining CUNY, Dr. Fazio was a postdoctoral fellow in the Content Protection group at IBM Almaden Research Center and a visiting researcher in the Cryptography Research group at IBM T.J. Watson Research center.

2 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.

3 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.

4 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.

5 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.

6 Course Textbook

- *Introduction to Modern Cryptography* by Jonathan Katz and Yehuda Lindell. Chapman & Hall/CRC Press, 2007.

7 Course Topics

- **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.

- **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.
  - ϵ-universal, universal one-way, and collision resistant hash functions. Merkle-Damgaard construction.
  - The hash-the-MAC paradigm.

- **Computationally Secure Symmetric Cryptography**
  - Definition of secure symmetric encryption: IND, CPA, CCA.
  - Block-ciphers and mode of operations.
  - Message authentication codes.
  - Hash-then-authenticate paradigm.

- **Managing Shared Keys**
  - The key distribution problem
  - Diffie-Hellman Key Exchange

- **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.

- **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.

- A taste of more advanced topics (identification schemes, commitment schemes, secret sharing).

8 Assessment

Grade will be based on:

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