

CSC Modern Cryptography

Professor Nelly Fazio

In this introductory, graduate-level course we introduce 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.

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

Textbook:

"Introduction to Cryptography", by Jonathan Katz and Yehuda Lindell