CS 7301.002 Advanced Cryptography
Recent Advances in Computing

Yvo Desmedt

1 Aim

Security proofs (based on reduction and on the random oracle model) play a primordial role in modern cryptography. The goal is to make the students familiar with such proofs. Students will be able to read most modern papers on cryptography after having taken this course.

2 Outline

Security Definitions, Proven Security, Random Oracle, Standard Reduction, Models, Chosen Text Attack, Non-Malleability, Diffie-Hellman Assumptions, Universal Hash Functions, Universal One-Way Hash Functions, Cramer-Shoup encryption, Block Ciphers (Luby-Rackoff), Pseudo-Random Generators, Pseudo-Random Functions (Naor- Reingold), Proven Secure Digital Signatures, Oblivious Transfer, Secure Multiparty Computation, Proven Secure Modes of Encryption/Authentication, Post-Quantum Cryptography

3 Background

Students are supposed to have taken CS6377 Introduction to Cryptography. Students who are not familiar with the background material, need to familiarize themselves with the background material. See https://dox.utdallas.edu/syl136031 and https://coursebook.utdallas.edu/search/cs6377.001.23f for details.