Course Document for Introduction to Cryptography

Somesh Jha
Computer Sciences Department
University of Wisconsin
Madison, WI 53706.
email: jha@cs.wisc.edu

This is an introductory course on cryptography.

This course serves as an undergraduate introduction to cryptography. The aim is to understand the theoretical foundations for cryptosystems used in the real world. This course is cross-listed with the mathematics department, so it will have a significant mathematical component. No advanced mathematics background is assumed, but students are expected to possess ”mathematical maturity” since many of the concepts will be abstract, rigorous definitions and proofs will be given, and we will cover some advanced mathematics (group theory, number theory) in class. Some background in discrete mathematics (probability theory, modular arithmetic) and algorithms will be helpful, but all necessary prerequisites will be reviewed in class.

0.1 Book

The required text for this class is given below.

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

1 Grading criteria (Not Finalized)

- **Homeworks (30%):** 6-8 homeworks will be assigned.
- **Exams (70%):** A midterm exam (30% total), and a final exam (40%).