Introduction to Modern Cryptography

Mihir Bellare[1] **Phillip Rogaway**[2]

September 21, 2005

[1] Department of Computer Science and Engineering, University of California at San Diego, La Jolla, CA 92093, USA. mihir@cs.ucsd.edu, http://www-cse.ucsd.edu/users/mihir

[2] Department of Computer Science, Kemper Hall of Engineering, University of California at Davis, Davis, CA 95616, USA; and Department of Computer Science, Faculty of Science, Chiang Mai University, Chiang Mai, 50200 Thailand. rogaway@cs.ucdavis.edu, http://www.cs.ucdavis.edu/∼rogaway

Preface

This is a set of class notes that we have been developing jointly for some years. We use them for cryptography courses that we teach at our respective institutions. Each time one of us teaches the class, he takes the token and updates the notes a bit. The process has resulted in an evolving document that has lots of gaps, as well as plenty of "unharmonized" parts. One day it will, with luck, be complete and cogent.

The viewpoint taken throughout these notes is to emphasize the *theory of cryptography as it can be applied to practice.* This is an approach that the two of us have pursued in our research, and it seems to be a pedagogically desirable approach as well.

We would like to thank the following students of past versions of our courses who have pointed out errors and made suggestions for changes: Andre Barroso, Keith Bell, Kostas Bimpikis, Alexandra Boldyreva, Dustin Boswell, Brian Buesker, Michael Burton, Chris Calabro, Sashka Davis, Alex Gantman, Bradley Huffaker, Hyun Min Kang, Vivek Manpuria, Chanathip Namprempre, Adriana Palacio, Wenjing Rao, Fritz Schneider, Juliana Wong. We welcome further corrections, comments and suggestions.

Mihir Bellare San Diego, California USA
Phillip Rogaway Davis, California USA