

Introduction to Modern Cryptography

Mihir Bellare¹

Phillip Rogaway²

November 3, 2003

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, Alexandra Boldyreva, Brian Buesker, Michael Burton, Chris Calabro, Sashka Davis, Alex Gantman, Bradley Huffaker, Vivek Manpuria, Chanathip Namprempre, Adriana Palacio, Wenjing Rao, Fritz Schneider, Juliana Wong. We welcome further corrections, comments and suggestions.

Mihir Bellare
Phillip Rogaway

San Diego, California USA
Davis, California USA

©Mihir Bellare and Phillip Rogaway, 1997–2003.

Contents

1	INTRODUCTION	7
1.1	Goals and settings	8
1.2	Settings and goals	9
1.3	Other goals	16
1.4	What cryptography is about	18
1.5	Approaches to the study of cryptography	21
1.6	What background do I need?	30
1.7	Historical notes	31
1.8	Problems	31
2	BLOCK CIPHERS	33
2.1	What is a block cipher?	33
2.2	Data Encryption Standard (DES)	34
2.3	Advanced Encryption Standard (AES)	37
2.4	Some modes of operation	41
2.5	Key recovery attacks on block ciphers	43
2.6	Limitations of key-recovery based security	45
2.7	Problems	46
3	PSEUDORANDOM FUNCTIONS	49
3.1	Function families	49
3.2	Random functions and permutations	50
3.3	Pseudorandom functions	56
3.4	Pseudorandom permutations	59
3.5	Usage of PRFs and PRPs	62
3.6	Example Attacks	65
3.7	Security against key recovery	68
3.8	The birthday attack	74
3.9	The PRP/PRF switching lemma	75
3.10	Unix one-way function	80
3.11	Pseudorandom generators	85
3.12	Historical notes	85

3.13	Problems	86
4	SYMMETRIC ENCRYPTION	89
4.1	Symmetric encryption schemes	89
4.2	Example encryption schemes (ECB, CBC, CTR)	91
4.3	Issues in privacy	97
4.4	Indistinguishability under chosen-plaintext attack	99
4.5	Example chosen-plaintext attacks	104
4.6	Notions equivalent to indistinguishability	108
4.7	Indistinguishability implies security against plaintext recovery	114
4.8	Indistinguishability from random bits implies indistinguishability	118
4.9	Security of CTR modes	121
4.10	Security of CBC with a random IV	124
4.11	Indistinguishability under chosen-ciphertext attack	130
4.12	Example chosen-ciphertext attacks	132
4.13	Historical notes	136
4.14	Problems	137
5	HASH FUNCTIONS	139
5.1	Collision-resistant hash functions	139
5.2	One-wayness of collision-resistant hash functions	142
5.3	The MD transform	146
5.4	Collision-resistance under hidden-key attack	147
5.5	Problems	148
6	MESSAGE AUTHENTICATION	149
6.1	The setting	149
6.2	Privacy does not imply authenticity	152
6.3	Syntax of message-authentication schemes	153
6.4	A definition of security for MACs	155
6.5	Examples	161
6.6	The PRF-as-a-MAC paradigm	164
6.7	The CBC MACs	166
6.8	Problems	167
7	AUTHENTICATED ENCRYPTION	169
8	COMPUTATIONAL NUMBER THEORY	171
8.1	The basic groups	171
8.2	Algorithms	173
8.3	Cyclic groups and generators	179
8.4	Squares and non-squares	184
8.5	Groups of prime order	189

8.6	Historical Notes	191
8.7	Exercises and Problems	191
9	NUMBER-THEORETIC PRIMITIVES	193
9.1	Discrete logarithm related problems	193
9.2	The choice of group	199
9.3	The RSA system	202
9.4	Historical notes	206
9.5	Exercises and Problems	206
10	ASYMMETRIC ENCRYPTION	207
10.1	Asymmetric encryption schemes	208
10.2	Notions of security	209
10.3	One encryption query or many?	214
10.4	Hybrid encryption	217
10.5	El Gamal scheme and its variants	230
11	DIGITAL SIGNATURES	237
11.1	Digital signature schemes	237
11.2	A notion of security	239
11.3	RSA based signatures	240
12	AUTHENTICATED KEY EXCHANGE	261
13	THE ASYMPTOTIC APPROACH	263
14	INTERACTIVE PROOFS AND ZERO KNOWLEDGE	265
14.1	Introduction	265
14.2	Interactive functions and the accepting probability	270
14.3	Proofs of language-membership	272
14.4	NP proof-systems	277
14.5	Exercises and Problems	278
A	THE BIRTHDAY PROBLEM	279
B	INFORMATION-THEORETIC SECURITY	283

