

# A COURSE IN CRYPTOGRAPHY

RAFAEL PASS  
ABHI SHELAT

© 2010 Pass/shelat  
All rights reserved Printed online

11 11 11 11 11    15 14 13 12 11 10 9

First edition:    June 2007  
Second edition:    September 2008  
Third edition:    January 2010

# Contents

|   |            |
|---|------------|
| <b>Contents</b>                                       | <b>i</b>   |
| <b>Algorithms &amp; Protocols</b>                     | <b>v</b>   |
| <b>List of Major Definitions</b>                      | <b>vi</b>  |
| <b>Preface</b>  | <b>vii</b> |
| <b>Numbering and Notation</b>                         | <b>ix</b>  |
| <b>1 Introduction</b>                                 | <b>1</b>   |
| 1.1 Classical Cryptography: Hidden Writing . . . . .  | 1          |
| 1.2 Modern Cryptography: Provable Security . . . . .  | 6          |
| 1.3 Shannon’s Treatment of Provable Secrecy . . . . . | 10         |
| 1.4 Overview of the Course . . . . .                  | 19         |
| <b>2 Computational Hardness</b>                       | <b>21</b>  |
| 2.1 Efficient Computation and Efficient Adversaries . | 21         |
| 2.2 One-Way Functions . . . . .                       | 26         |
| 2.3 Multiplication, Primes, and Factoring . . . . .   | 29         |
| 2.4 Hardness Amplification . . . . .                  | 34         |
| 2.5 Collections of One-Way Functions . . . . .        | 41         |
| 2.6 Basic Computational Number Theory . . . . .       | 42         |
| 2.7 Factoring-based Collection of OWF . . . . .       | 51         |
| 2.8 Discrete Logarithm-based Collection . . . . .     | 51         |
| 2.9 RSA Collection . . . . .                          | 53         |
| 2.10 One-way Permutations . . . . .                   | 55         |
| 2.11 Trapdoor Permutations . . . . .                  | 56         |
| 2.12 Rabin collection . . . . .                       | 57         |

|          |  |            |
|----------|--|------------|
| 2.13     | A Universal One Way Function . . . . .                 | 63         |
| <b>3</b> | <b>Indistinguishability &amp; Pseudo-Randomness</b>    | <b>67</b>  |
| 3.1      | Computational Indistinguishability . . . . .           | 68         |
| 3.2      | Pseudo-randomness . . . . .                            | 74         |
| 3.3      | Pseudo-random generators . . . . .                     | 77         |
| 3.4      | Hard-Core Bits from Any OWF . . . . .                  | 83         |
| 3.5      | Secure Encryption . . . . .                            | 91         |
| 3.6      | An Encryption Scheme with Short Keys . . . . .         | 92         |
| 3.7      | Multi-message Secure Encryption . . . . .              | 93         |
| 3.8      | Pseudorandom Functions . . . . .                       | 94         |
| 3.9      | Construction of Multi-message Secure Encryption        | 99         |
| 3.10     | Public Key Encryption . . . . .                        | 101        |
| 3.11     | El-Gamal Public Key Encryption scheme . . . . .        | 105        |
| 3.12     | A Note on Complexity Assumptions . . . . .             | 107        |
| <b>4</b> | <b>Knowledge</b>                                       | <b>109</b> |
| 4.1      | When Does a Message Convey Knowledge . . . . .         | 109        |
| 4.2      | A Knowledge-Based Notion of Secure Encryption          | 110        |
| 4.3      | Zero-Knowledge Interactions . . . . .                  | 113        |
| 4.4      | Interactive Protocols . . . . .                        | 114        |
| 4.5      | Interactive Proofs . . . . .                           | 116        |
| 4.6      | Zero-Knowledge Proofs . . . . .                        | 120        |
| 4.7      | Zero-knowledge proofs for NP . . . . .                 | 124        |
| 4.8      | Proof of knowledge . . . . .                           | 130        |
| 4.9      | Applications of Zero-knowledge . . . . .               | 130        |
| <b>5</b> | <b>Authentication</b>                                  | <b>133</b> |
| 5.1      | Message Authentication . . . . .                       | 133        |
| 5.2      | Message Authentication Codes . . . . .                 | 134        |
| 5.3      | Digital Signature Schemes . . . . .                    | 135        |
| 5.4      | A One-Time Signature Scheme for $\{0, 1\}^n$ . . . . . | 136        |
| 5.5      | Collision-Resistant Hash Functions . . . . .           | 139        |
| 5.6      | A One-Time Digital Signature Scheme for $\{0, 1\}^*$   | 144        |
| 5.7      | *Signing Many Messages . . . . .                       | 145        |
| 5.8      | Constructing Efficient Digital Signature . . . . .     | 148        |
| 5.9      | Zero-knowledge Authentication . . . . .                | 149        |
| <b>6</b> | <b>Computing on Secret Inputs</b>                      | <b>151</b> |

|          |  |            |
|----------|--|------------|
| 6.1      | Secret Sharing . . . . .                           | 151        |
| 6.2      | Yao Circuit Evaluation . . . . .                   | 154        |
| 6.3      | Secure Computation . . . . .                       | 164        |
| <b>7</b> | <b>Composability</b>                               | <b>167</b> |
| 7.1      | Composition of Encryption Schemes . . . . .        | 167        |
| 7.2      | Composition of Zero-knowledge Proofs* . . . . .    | 175        |
| 7.3      | Composition Beyond Zero-Knowledge Proofs . . . . . | 178        |
| <b>8</b> | <b>*More on Randomness and Pseudorandomness</b>    | <b>179</b> |
| 8.1      | A Negative Result for Learning . . . . .           | 179        |
| 8.2      | Derandomization . . . . .                          | 180        |
| 8.3      | Imperfect Randomness and Extractors . . . . .      | 181        |
|          | <b>Bibliography</b>                                | <b>185</b> |
| <b>A</b> | <b>Background Concepts</b>                         | <b>187</b> |
| <b>B</b> | <b>Basic Complexity Classes</b>                    | <b>191</b> |

[Click here to download full PDF material](#)