CSCI 1515: Applied Cryptography

P. Miao

Spring 2023

These are lecture notes for CSCI 1515: Applied Cryptography taught at Brown University by Peihan Miao in the Spring of 2023.

These notes are taken by Jiahua Chen with gracious help and input from classmates. Please direct any mistakes/errata to me via email, post a thread on Ed, or feel free to pull request or submit an issue to the notes repository (https://github.com/BrownAppliedCryptography/notes).

FYI, todo's are marked like this.

Notes last updated February 7, 2023.

Contents

1 January 26, 2023 **3**
1.1 Introduction . . . 3
1.2 Course Logistics . . . 3
1.3 What is cryptography? . . . 4
1.4 Secure Communication . . . 5
1.4.1 Message Secrecy . . . 6
1.4.2 Message Integrity . . . 8
1.5 Project Overview . . . 10
1.5.1 Zero-Knowledge Proofs . . . 10
1.5.2 Secure Multi-Party Computation . . . 12
1.5.3 Fully Homomorphic Encryption . . . 14
1.5.4 Further Topics . . . 16
1.6 A Quick Survey . . . 17

2 January 31, 2023 **18**
2.1 Logistics . . . 18
2.2 Encryption Schemes . . . 18
2.2.1 Syntax . . . 19
2.2.2 Symmetric-Key Encryption Schemes . . . 20
2.2.3 Public-Key Encryption Schemes . . . 26
2.2.4 RSA . . . 29

3 February 2, 2023 **31**
3.1 RSA Encryption, *continued* . . . 31

3.2 Intro to Group Theory . . . 33
3.3 Computational Assumptions . . . 34
3.4 ElGamal Encryption . . . 34
3.5 Secure Key Exchange . . . 35
3.6 Message Integrity . . . 36
3.6.1 Syntax . . . 38
3.6.2 Chosen-Message Attack . . . 38
3.6.3 Constructions . . . 39

4 February 7, 2023 **40**
4.1 Message Integrity, *reviewed* . . . 40
4.1.1 Message Authentication Code . . . 40
4.1.2 Digital Signature . . . 40
4.1.3 Syntax . . . 41
4.1.4 Constructions . . . 41
4.2 RSA Signatures . . . 42
4.3 DSA Signatures . . . 43
4.4 Authenticated Encryption . . . 43
4.4.1 Encrypt-and-MAC? . . . 45
4.4.2 Encrypt-then-MAC . . . 46
4.4.3 MAC-then-Encrypt . . . 46
4.4.4 Chosen Ciphertext Attack Security . . . 47
4.5 A Summary So Far . . . 47
4.6 Hash Function . . . 48
4.6.1 Random Oracle Model . . . 49
4.6.2 Constructions for Hash Function . . . 50