COMP4109 Final Exam Practice

William Findlay

December 6, 2019

Contents

List of Figures

List of Tables

List of Listings

1 List of Topics

Table 1.1: Topics for the final with percentages and approximate number of questions. N.b. total number of questions is 44, but total approximate only adds up to 39.

Topic	Percentage	≈ Questions
Classical Crypto	(10%)	4
Secret Key Crypto	(10%)	4
Security Models and Goals	(18%)	8
Public Key Crypto and Efficiency	(15%)	7
Hash Functions	(7%)	3
Hashes/MACs/DSS	(10%)	4
Secret Sharing	(2%)	1
WEP	(5%)	2
Secure Internet Connections	(10%)	4
Zero Knowledge Proofs	(5%)	2

2 Notes

2.1 Midterm 1

2.1.1 Classical Crypto

2.1.2 Secret Key Crypto

2.1.3 Security Models and Goals

2.2 Midterm 2

2.2.1 Public Key Crypto

2.2.2 Hash Functions

2.2.3 Hashes/MACs/DSS

2.3 Post-Midterms

2.3.1 Secret Sharing

2.3.2 WEP

2.3.3 Secure Internet Connections

2.3.4 Zero Knowledge Proofs

3 Practice Questions

3.1 Provided Multiple Choice Questions

3.2 Custom Multiple Choice Questions