

# COMP4109 Final Exam Practice

*William Findlay*

*December 6, 2019*

# Contents

<b>1</b>	<b>List of Topics</b>	<b>1</b>
<b>I</b>	<b>Notes</b>	<b>1</b>
<b>2</b>	<b>Midterm 1</b>	<b>2</b>
2.1	Classical Crypto . . . . .	2
2.2	Secret Key Crypto . . . . .	2
2.3	Security Models and Goals . . . . .	2
<b>3</b>	<b>Midterm 2</b>	<b>2</b>
3.1	Public Key Crypto . . . . .	2
3.2	Hash Functions . . . . .	2
3.3	Hashes/MACs/DSS . . . . .	2
<b>4</b>	<b>Post-Midterms</b>	<b>2</b>
4.1	Secret Sharing . . . . .	2
4.2	WEP . . . . .	2
4.3	Secure Internet Connections . . . . .	2
4.4	Zero Knowledge Proofs . . . . .	2
<b>II</b>	<b>Practice Questions</b>	<b>2</b>
<b>5</b>	<b>Provided Multiple Choice Questions</b>	<b>2</b>
<b>6</b>	<b>Custom Multiple Choice Questions</b>	<b>2</b>

## List of Figures

## List of Tables

1.1	Topics for the final . . . . .	1
-----	--------------------------------	---

## 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	$\approx$ 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

## Part I

# Notes

## 2 Midterm 1

### 2.1 Classical Crypto

### 2.2 Secret Key Crypto

### 2.3 Security Models and Goals

## 3 Midterm 2

### 3.1 Public Key Crypto

### 3.2 Hash Functions

### 3.3 Hashes/MACs/DSS

## 4 Post-Midterms

### 4.1 Secret Sharing

### 4.2 WEP

### 4.3 Secure Internet Connections

### 4.4 Zero Knowledge Proofs

## Part II

# Practice Questions

## 5 Provided Multiple Choice Questions

## 6 Custom Multiple Choice Questions