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

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

1. A stream cipher provides which of the following?
   (a) Indistinguishability
   (b) Unpredictability
   (c) Synchronicity
   (d) **A and B**

(e) None of the above

2. The security of RSA is believed to be based on...
   (a) **The difficulty of factoring the modulus**
   (b) The computational DH problem
   (c) The discrete log problem
   (d) B and C
   (e) None of the above

3. What is 17^{122} mod 23?
   (a) 17×122 mod 23
   (b) 17^7 mod 23
   (c) $\mathbf{17^{12}}$ **mod 23**
   (d) 17^{12} mod 22
   (e) None of the above

4. Consider the following ciphertext $c =$ wud. The shift (Caesar) cipher was used. What is the plaintext?
   (a) foo
   (b) the
   (c) ack
   (d) **gen**
   (e) None of the above

5. Changing a single bit of the plaintext should change about 1/2 the bits of the ciphertext? What security goal is this?
   (a) **Diffusion**
   (b) Confusion
   (c) Unpredictability
   (d) Non-Malleability
   (e) None of the above

6. What information does a collision reveal when using ECB (electronic code book)? When $c_i = c_j$, what do we know?
   (a) It will leak information about the plaintext
   (b) It reveals the contents of all the blocks
   (c) It causes an existential forgery
   (d) It leaks information about the secret key
   (e) **None of the above**

7. Which of the following does a MAC provide that a hash function does not?
   (a) Data origin authentication (anyone)
   (b) Data integrity authentication (those with the key)
   (c) **Data origin authentication (those with the key)**
   (d) Non-repudiation (those with the key)
   (e) None of the above

8. Assume the padding scheme outlined in class for CBC mode. The cipher has block length 2 bytes. How do we pad the following plaintext? `a1 b2 33 12`
   (a) Append `0a` 4 times
   (b) **Append `0a` 2 times**
   (c) Append `00` 2 times
   (d) Do nothing
   (e) None of the above

For the next two questions, consider the following connection encrypted line:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2
```

9. Which digital signature scheme is used?
   (a) ECDHE
   (b) RSA
   (c) AES
   (d) **SHA384**
   (e) None of the above

10. Which security protocol is used?
   (a) ECDHE
   (b) **TLS 1.2**
   (c) AES
   (d) GCM
   (e) None of the above

6 Custom Multiple Choice Questions