COMP4109 Final Exam Practice

William Findlay

December 7, 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

- security goals
  - ▶ confidentiality (nope)
  - ▶ access control (nope)
  - ▶ data integrity (nope)
- how it works
  - ▶ random 24-bit IV v
  - ▶ compute 32-bit checksum of m
  - ▶ $c = \text{RC4}(v, k) \oplus (m||\text{checksum}(m))$
- many problems
  - ▶ RC4(v, k) not good due to k and v themselves (without even exploiting how crappy RC4 is)
    - ◦ really only depends on v
    - ◦ because k rarely changes and is often shared by everyone in LAN
    - ◦ guaranteed collision in v after ≈ 16 millions transmissions
    - ◦ birthday attack on random v only needs 4096
    - ◦ v often tracked with counter and reset when device is started
    - ◦ so small $v \implies$ lots of collisions
  - ▶ collision + KPA means:

- if we have $< v, c >$, we can decrypt $< v, c' >$ if we can find a collision in v

- decryption dictionary
  - RC4(v_i, k), watch transmissions in the network
  - full dictionary only needs 24GB of space
- malleability
  - message modification is easy since checksums suck
  - only good at detecting one or two flipped bits, errors can cancel each other
- authentication spoofing
  - base station sends plaintext challenge z
  - client sends back the WEP encryption of z
  - observer has the plaintext, ciphertext pair for free
- double encryption
  - you can just send q to yourself from another station
  - oracle encrypts $q', v' = \text{WEP}(q)$
  - if $v = v'$, we can decrypt q' to q

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) $17^7 \bmod 23$
(c) $17^{12} \bmod 23$
(d) $17^{12} \bmod 22$
(e) None of the above

4. Consider the following ciphertext $c = \text{wud}$. 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

1. Which of the following is not a security flaw in WEP?
   (a) Easy to find collisions in v
   (b) k is often shared across the entire LAN
   (c) An attacker can mount a chosen plaintext attack by sending m to himself
   (d) An attacker can mount a known plaintext attack by finding a collision in v
   (e) All of the above are security flaws in WEP

2. How does WEP encrypt messages?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

3. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

4. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

5. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

6. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

7. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

8. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

9. This is a template question?
   (a)
   (b)
   (c)
   (d)
   (e) None of the above

10. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

11. This is a template question?
    (a)
    (b)
    (c)

(d)
(e) None of the above

12. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

13. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

14. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

15. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

16. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

17. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

18. This is a template question?

(a)
(b)
(c)
(d)
(e) None of the above

19. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

20. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

21. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

22. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

23. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

24. This is a template question?
    (a)
    (b)
    (c)
    (d)

(e) None of the above

25. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

26. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

27. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

28. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

29. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

30. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

31. This is a template question?
    (a)

(b)
(c)
(d)
(e) None of the above

32. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

33. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

34. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

35. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

36. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

37. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

38. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

39. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

40. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

41. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

42. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

43. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

44. This is a template question?
    (a)
    (b)
    (c)

(d)
(e) None of the above

45. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

46. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

47. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

48. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

49. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

50. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

51. This is a template question?

(a)
(b)
(c)
(d)
(e) None of the above

52. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

53. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

54. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

55. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

56. This is a template question?
(a)
(b)
(c)
(d)
(e) None of the above

57. This is a template question?
(a)
(b)
(c)
(d)

(e) None of the above

58. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

59. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above

60. This is a template question?
    (a)
    (b)
    (c)
    (d)
    (e) None of the above