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 `02` 4 times
   (b) Append `02` 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) $\text{RC4}(\text{checksum}(m), k) \oplus (v||m)$
   (b) WEP does not encrypt messages
   (c) $\text{RSA}(v, k) \oplus (m||\text{checksum}(m))$
   (d) $\text{RC4}(v, k) \oplus (m||\text{checksum}(m))$
   (e) None of the above

3. Which security goal of WEP is broken by the ability to easily find collisions in v?
   (a) Indistinguishability
   (b) Confidentiality
   (c) Access control
   (d) Data integrity
   (e) None of the above

4. How many bits is v in WEP?
   (a) 32
   (b) 8
   (c) 48
   (d) 24
   (e) None of the above

5. How many bits is the checksum in WEP?
   (a) 32
   (b) 8
   (c) 48
   (d) 24
   (e) None of the above

6. Why are checksums not a good choice for data integrity in WEP?
   (a) Vulnerable to an addition attack
   (b) Easily malleable
   (c) Errors can cancel
   (d) B and C
   (e) None of the above

7. Which of the following is not a security goal of WEP?
   (a) Confidentiality
   (b) Data integrity
   (c) Indistinguishability
   (d) Access control
   (e) None of the above

8. What is the definition of a symmetric key encryption scheme?
   (a) Three efficient algorithms: G, E_e, D_d
   (b) Five-tuple: K, P, C, E, D
   (c) An encryption scheme where the key is always the same size
   (d) Three-tuple: K, P, C
   (e) None of the above

9. A _____ allows us to encrypt messages longer than the plaintext length.
   (a) Symmetric key encryption scheme
   (b) Block cipher
   (c) Mode of operation
   (d) Public key encryption scheme
   (e) None of the above

10. What is the plaintext length in an unmodified Caesar cipher?
    (a) The key length
    (b) Any size
    (c) 26
    (d) 1
    (e) None of the above

11. What is the plaintext length in an unmodified Vigenère cipher?
    (a) The key length
    (b) Any size
    (c) 26

(d) 1
(e) None of the above

12. How is a Vigenère cipher similar to one-time pad?
    (a) One-time pad is like Vigenère except it has key length = plaintext length
    (b) They are the same thing
    (c) One-time pad is like Vigenère except the key changes each time
    (d) A and C
    (e) None of the above

13. The one-time pad _____.
    (a) Is unconditionally secure
    (b) Provides perfect secrecy
    (c) Is extremely efficient
    (d) A and B
    (e) None of the above

14. Which of the following is a problem with the one time pad?
    (a) It is malleable
    (b) It is vulnerable to chosen plaintext attacks
    (c) It can only be used for very large messages
    (d) The keyspace is finite
    (e) None of the above

15. Which of the following symmetric key encryption schemes provides information theoretic security IND-KPA?
    (a) AES in CBC mode
    (b) Affine cipher
    (c) One-time pad
    (d) AES in CTR mode
    (e) None of the above

16. Which of the following is not a security goal?
    (a) Non-malleability
    (b) Access control
    (c) Indistinguishability
    (d) Data integrity
    (e) All of the above **are** security goals

17. Which of the following is not an attack model?
    (a) Known plaintext attack
    (b) Chosen plaintext attack
    (c) Ciphertext only attack
    (d) Chosen message attack
    (e) All of the above **are** attack models

18. Which of the following is not a security level?
    (a) Complexity theoretic
    (b) Polynomial
    (c) Computational
    (d) Information theoretic
    (e) All of the above **are** security levels

19. An attacker knows one or more plaintext, ciphertext pairs and tries to find k. What attack is this?
    (a) Chosen plaintext attack
    (b) Ciphertext only attack
    (c) Known plaintext attack
    (d) Ciphertext stealing
    (e) None of the above

20. An attacker has access to an oracle that can encrypt messages. What attack is this?
    (a) Chosen plaintext attack
    (b) Ciphertext only attack
    (c) Known plaintext attack
    (d) Ciphertext stealing
    (e) None of the above

21. An attacker tries to decrypt ciphertext with no other information. What attack is this?
    (a) Chosen plaintext attack
    (b) Ciphertext only attack
    (c) Known plaintext attack
    (d) Ciphertext stealing
    (e) None of the above

22. Which of the following best describes unicity distance?
    (a) The number of times you have to encrypt random plaintext before getting a collision in the ciphertext
    (b) The theoretical complexity difference between two encryption schemes
    (c) The expected minimum ciphertext length required to uniquely compute the key
    (d) The size of a given ciphertext space
    (e) None of the above

23. What is a spurious key?
    (a) A key that does not exist in our keyspace
    (b) A key that uniquely maps plaintext to a given ciphertext
    (c) Another key that decrypts ciphertext to an alternative, yet valid, plaintext
    (d) A key that results in gibberish decryption
    (e) None of the above

24. If $c =$ `Dpssphtzbe` is the ciphertext generated by one-time pad, what is the corresponding plaintext?

(a) `Andybuigod`
(b) `Triisgreat`
(c) `Williamsux`
(d) `Amandabest`
(e) Not enough information

25. If $c =$ `Dpssphtzbe` is the ciphertext generated by one-time pad, what is the corresponding plaintext?
    (a) `Andybuigod`
    (b) `Triisgreat`
    (c) `Williamsux`
    (d) `Amandabest`
    (e) Not enough information

26. Which of the following is the current standard for block ciphers?
    (a) 2DES
    (b) 3DES
    (c) AES
    (d) DES
    (e) None of the above

27. A meet in the middle attack reduces 2DES from _____ to _____.
    (a) An NP-Hard problem, a P problem
    (b) 128 bit block length, 112 bit effective block length
    (c) 112 bit block length, 57 bit effective block length
    (d) 64 bit block length, 60 bit effective block length
    (e) None of the above

28. A meet in the middle attack reduces 3DES from _____ to _____.
    (a) An NP-Complete problem, an NP-Hard problem
    (b) 168 bit block length, 57 bit effective block length
    (c) 256 bit block length, 128 bit effective block length
    (d) 168 bit block length, 112 bit effective block length
    (e) None of the above

29. DES suffers from _____.
    (a) Inefficient encryption
    (b) Short block length
    (c) Long key length
    (d) B and C
    (e) None of the above

30. 3DES works by doing which of the following?
    (a) $D_{k_3}(D_{k_2}(E_{k_1}(m)))$
    (b) $D_{k_3}(E_{k_2}(D_{k_1}(m)))$
    (c) $E_{k_3}(E_{k_2}(E_{k_1}(m)))$

(d) $E_{k_3}(D_{k_2}(E_{k_1}(m)))$
(e) None of the above

31. 2DES works by doing which of the following?
    (a) $E_{k_2}(D_{k_1}(m))$
    (b) $D_{k_2}(D_{k_1}(m))$
    (c) $E_{k_2}(E_{k_1}(m))$
    (d) $D_{k_2}(E_{k_1}(m))$
    (e) None of the above

32. In 3DES, which of the following are possible?
    (a) $k_1 \neq k_2 \neq k_3$
    (b) $k_1 = k_2 = k_3$
    (c) $k_1 \neq k_2, k_2 = k_3$
    (d) A and B
    (e) All of the above

33. According to the PKCS#7 padding scheme we saw in class, how would you pad `ae 12 64` with a block length of 6 bytes?
    (a) `ae 12 64 06 06 06`
    (b) `06 06 06 ae 12 64`
    (c) `ae 12 64 03 03 03`
    (d) `03 03 03 ae 12 64`
    (e) None of the above

34. According to the PKCS#7 padding scheme we saw in class, how would you pad `ae 12 64` with a block length of 3 bytes?
    (a) `ae 12 64`
    (b) `03 03 03 ae 12 64`
    (c) `ae 12 64 03 03 03`
    (d) `ae 12 64 00 00 00`
    (e) None of the above

35. Ciphertext stealing works with which of the following modes of operation?
    (a) CBC
    (b) GCM
    (c) ECB
    (d) CTR
    (e) None of the above

36. Which mode of operation has no semantic security?
    (a) CBC
    (b) GCM
    (c) ECB
    (d) CTR
    (e) None of the above

37. CTR mode generates keys by _____.
    (a) Encrypting an increasing value each time, starting at zero
    (b) Incrementing and then encrypting a nonce each time
    (c) Decrementing a nonce, encrypting it, and then incrementing it each time
    (d) Encrypting a nonce and then incrementing it each time
    (e) None of the above

38. How does CTR mode generate ciphertext?
    (a) Each block of plaintext is XORed with the encrypted nonce
    (b) Each plaintext block is encrypted using the nonce as a key
    (c) Each block of plaintext is XORed with the previous ciphertext and then encrypted
    (d) Each plaintext block is run through the encryption algorithm and then XORed with the nonce
    (e) None of the above

39. Which of the following describes ECB?
    (a) Block length does not matter
    (b) Encrypt each block individually
    (c) Computationally IND-CPA secure
    (d) ECB is technically a stream cipher
    (e) None of the above

40. Which of the following describes CBC?
    (a) Suffers from a lack of diffusion
    (b) Vulnerable to meet in the middle attacks
    (c) XOR plaintext block with previous ciphertext block and then encrypt
    (d) Does not require padding
    (e) None of the above

41. In ciphertext stealing we do which of the following?
    (a) Pad last block with `0`s until it meets block length, encrypt as normal, then swap first and last blocks
    (b) Pad last block with `1`s until it meets block length, encrypt as normal, then swap first and last blocks
    (c) Pad last block with `1`s until it meets block length, encrypt as normal, then swap last two blocks
    (d) Pad last block with `0`s until it meets block length, encrypt as normal, then swap last two blocks
    (e) None of the above

42. What is $33^{89} \bmod 45$?
    (a) 33
    (b) 37
    (c) $33^{44} \bmod 45$
    (d) 1

(e) None of the above

43. Which of the following is in the correct order of reducibility?
    (a) DL > DDH > CDH
    (b) DL > CDH > DDH
    (c) DDH > CDH > DL
    (d) CDH > DDH > DL
    (e) None of the above

44. Which of the following describes the CDH problem?
    (a) Given (p, g, g^a, g^b, n), try to determine if $n = g^{ab} \bmod p$ or $n = g^x \bmod p$
    (b) Given (p, g, g^a), try to find $a \bmod p$.
    (c) Given (p, g, g^a, g^b), try to compute $g^{ab} \bmod p$
    (d) Given (p, g, g^a, b), try to compute $g^{ab} \bmod p$
    (e) None of the above

45. Which of the following describes the DDH problem?
    (a) Given (p, g, g^a, g^b, n), try to determine if $n = g^{ab} \bmod p$ or $n = g^x \bmod p$
    (b) Given (p, g, g^a), try to find $a \bmod p$.
    (c) Given (p, g, g^a, g^b), try to compute $g^{ab} \bmod p$
    (d) Given (p, g, g^a, b), try to compute $g^{ab} \bmod p$
    (e) None of the above

46. Which of the following describes the DL problem?
    (a) Given (p, g, g^a, g^b, n), try to determine if $n = g^{ab} \bmod p$ or $n = g^x \bmod p$
    (b) Given (p, g, g^a), try to find $a \bmod p$.
    (c) Given (p, g, g^a, g^b), try to compute $g^{ab} \bmod p$
    (d) Given (p, g, g^a, b), try to compute $g^{ab} \bmod p$
    (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

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

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

(d)
(e) None of the above

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