COMP4109 Final Exam Practice

William Findlay

December 10, 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	(18%)	4
Security Models and Goals	(10%)	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 Symmetric-Key Encryption Definition

- Tuple (P,C,K,E,D)
  - P: Plaintext space
  - C: Ciphertext space
  - K: Keyspace
  - E: $e_k : \ P \to C$
  - D: $d_k : \ C \to P$

2.2 Classical Crypto

- Caesar Cipher
  - $E_k(m) = (m + k) mod 26$
  - $D_k(c) = (c - k) mod 26$
- Affine Cipher
  - $K = (a, b), \gcd(a, 26) = 1$
  - for $k = (a, b) \in K$
    - $E_k(m) = (am + b) \bmod 26$

    - $D_k(c) = a^{-1}(c - b) \bmod 26$
- Substitution Cipher
  - $A = \{a, b, c, ..., x, y, z\}$
  - K is set of all permutations of A
  - for $\pi \in K$
  - $E_k(m) = \pi m$
  - $D_k(c) = \pi^{-1} m$
- Vigenere cipher(polyalphabetic cipher)
  - K=$(\mathbb{Z}_{26})^{\ell}$
  - for $k = (k_1, k_2, ..., k_l)$ and $m = (m_1, m_2, ..., m_l) \in P$
  - $E_k(m_1, m_2, ..., m_l) = (m_1 + k_1, m_2 + k_2, ..., m_l + k_l) \bmod 26$
  - $D_k(c_1, c_2, ..., c_l) = (c_1 - k_1, c_2 - k_2, ..., c_l - k_l) \bmod 26$

2.3 Block Ciphers

2.4 Stream Ciphers

2.5 Symmetric Key Attack Models/Security Levels/Security Goals

2.5.1 Attack Models

- Ciphertext-only Attack (Passive attack)
  - Adversary is given C but not M
- Known-plaintext Attack (Passive attack)
  - Adversary knows one or more plaintext-ciphertext(M,C) pairs
- Chosen-plaintext attack(Active attack)
  - Adversary chooses M and is given C
- Chosen-ciphertext attack (Active attack)
  - Adversary chooses C and is given M

2.5.2 Security Levels

- Information-theoretic security
  - Adversary has no limits to their computational resources
- Complexity-theoretic security
  - Adversary has resources that are polynomial in the security parameter
- Computational security (Practical Security)
  - Adversary has n real computers at their disposal (computationally bounded)

2.5.3 Security Goals

- Indistinguishability
  - Ciphertexts should be indistinguishable from random strings
- Non-Malleability

- ▶ Can't modify C so that it decrypts to a new P that is meaningfully related to the original

2.6 Public Key Crypto Security Levels

- IND-CPA
  - ▶ indistinguishability given the adversary can encrypt arbitrary plaintext
- IND-CCA1
  - ▶ indistinguishability given the adversary can attempt to decrypt chosen ciphertext
- IND-CCA2
  - ▶ indistinguishability given the adversary can attempt to decrypt chosen ciphertext and adapt choices base don results

2.7 MACs Forgery

- existential forgery
  - ▶ there exists some forgery such that m' can be sent with the tag of m
- selective forgery
  - ▶ the attacker can choose some m' that can be sent with the tag of m
- universal forgery
  - ▶ the attacker can send any message they want with a valid tag

2.8 Security of Digital signatures, MACs, hash

- Digital signatures
  - ▶ data integrity (to anyone)
  - ▶ data origin authentication (to anyone)
  - ▶ non-repudiation
- MACs
  - ▶ data integrity (to other party with secret key)
  - ▶ data origin authentication (to other party with secret key)
- Hash
  - ▶ data integrity (to anyone)

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 $\approx$ 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 mod 23
   (c) 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 `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) RC4(checksum$(m), k) \oplus (v||m)$
   (b) WEP does not encrypt messages
   (c) RSA$(v, k) \oplus (m||$checksum$(m))$
   (d) RC4$(v, k) \oplus (m||$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 a Caesar cipher, 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 its XOR value 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 and counter
    (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 $20^{73} \bmod 37$?
    (a) 20
    (b) 37
    (c) $20^{36} \bmod 37$
    (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. The security of Diffie-Hellman relies on which of the following?
(a) Discrete log problem
(b) Computational Diffie-Hellman problem
(c) Decisional Diffie-Hellman problem
(d) B and C
(e) All of the above

48. In Diffie-Hellman, what is public information?
(a) g, p, g^a, g^b
(b) g, p, a, b
(c) g, p
(d) g^a, g^b
(e) None of the above

49. Which of the below corresponds to a vulnerability of Diffie-Hellman?
(a) Ciphertext stealing
(b) Existential forgery
(c) Meet in the middle
(d) Man in the middle
(e) None of the above

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

51. Which of the following is not a public key encryption scheme?
    (a) RSA
    (b) ElGamal
    (c) Diffie-Hellman
    (d) All of the above are public key encryption schemes
    (e) None of the above are public key encryption schemes

52. When $N = pq$, where p, q are prime, what is $\phi(N)$?
    (a) Undefined
    (b) $N - 1$
    (c) $(p - 1)(q - 1)$
    (d) 1
    (e) None of the above

53. When n is prime, what is $\phi(n)$?
    (a) Undefined
    (b) n
    (c) 0
    (d) $n - 1$
    (e) none of the above

54. How do we calculate e, d in RSA?
    (a) Find e, d such that $ed \equiv 1 \bmod \phi(N)$
    (b) Find e, d such that $ed \equiv 0 \bmod \phi(N)$
    (c) Find e, d such that $ed \equiv 0 \bmod N$
    (d) Find e, d such that $ed \equiv 1 \bmod N$
    (e) None of the above

55. How do we calculate N in RSA?
    (a) Take $N = ed$
    (b) Take $N = pq$ where p, q are two large random numbers
    (c) Take $N = pq$ where p, q are two large primes
    (d) Take N as some random large number
    (e) None of the above

56. Which of the following would yield m in RSA?
    (a) $(m^d)^e \bmod N$
    (b) $c^d \bmod \phi(N)$
    (c) $(m^e)^e \bmod N$
    (d) $(m^e)^d \bmod N$
    (e) None of the above

57. What is our public key in RSA?
    (a) (e, N)
    (b) (e, p, q)
    (c) $(e, \phi(N))$

(d) (d, N)
(e) None of the above

58. What is our private key in RSA?
    (a) $(d, \phi(N))$
    (b) (d, N)
    (c) (d, p, q)
    (d) (e, N)
    (e) None of the above

59. What is a generator in $\mathbb{Z}_p^*$?
    (a) Some integer in the group that can create every other group member when raised to various powers
    (b) Any member of the group
    (c) A way of creating other groups
    (d) The source of the group's power
    (e) None of the above

60. What is the cryptographic significance of the Euclidean Algorithm?
    (a) Helps us calculate N
    (b) Helps us calculate p, q
    (c) Helps us calculate $\phi(N)$
    (d) Forms the basis for Wiener's attack
    (e) None of the above

61. What is the cryptographic significance of the Extended Euclidean Algorithm?
    (a) Good for fast modular exponentiation
    (b) Helps us find modular inverse
    (c) Forms the basis for Wiener's attack
    (d) An integral part of the meet in the middle attack on 2DES
    (e) None of the above

62. Which of the following describes Wiener's attack?
    (a) Attempts to find k in ElGamal
    (b) Attempts to find d in RSA
    (c) Attempts to find p, q in RSA
    (d) Attempts to find a in ElGamal
    (e) None of the above

63. Generation in ElGamal involves which of the following?
    (a) Finding two primes p, q such that $p = 2q + 1$
    (b) Finding two random large primes
    (c) Computing a, b such that a, b are primitive elements in $\mathbb{Z}_p^*$
    (d) Finding e, d
    (e) None of the above

64. Generation in ElGamal involves which of the following?
    (a) Factoring the modulus
    (b) Finding a generator g in $\mathbb{Z}_p^*$ and computing $g^a \bmod p$ for random a
    (c) Finding a three-tuple of efficient equations
    (d) Finding a, b such that a and b are coprime
    (e) None of the above

65. What is a primitive element in $\mathbb{Z}_p^*$?
    (a) An element with order equal to the size of the group
    (b) An element equal to 1 mod p
    (c) A prime number in the group
    (d) The p in $\mathbb{Z}_p^*$
    (e) None of the above

66. What is a generator in $\mathbb{Z}_p^*$?
    (a) An element with order equal to the size of the group
    (b) An element equal to 1 mod p
    (c) A prime number in the group
    (d) The p in $\mathbb{Z}_p^*$
    (e) None of the above

67. What is $\phi(37)$?
    (a) 4
    (b) 38
    (c) 36
    (d) 12
    (e) None of the above

68. What is $\phi(45)$?
    (a) 44
    (b) 16
    (c) 24
    (d) 12
    (e) None of the above

69. Which of the following is not a security property of cryptographic hash functions?
    (a) Weak collision resistance
    (b) Preimage resistance
    (c) Collision resistance
    (d) Second preimage resistance
    (e) All of the above **are** security properties of cryptographic hash functions

70. Which of the following describes preimage resistance?
    (a) Hard to find any $m' \neq m$ such that $H(m) = H(m')$
    (b) Hard to find $m' \neq m$ given m such that $H(m) = H(m')$
    (c) Hard to find $H(H(m))$

(d) Hard to find m given $H(m)$
(e) None of the above

71. Which of the following describes second preimage resistance?
    (a) Hard to find any $m' \neq m$ such that $H(m) = H(m')$
    (b) Hard to find $m' \neq m$ given m such that $H(m) = H(m')$
    (c) Hard to find $H(H(m))$
    (d) Hard to find m given $H(m)$
    (e) None of the above

72. Which of the following describes collision resistance?
    (a) Hard to find any $m' \neq m$ such that $H(m) = H(m')$
    (b) Hard to find $m' \neq m$ given m such that $H(m) = H(m')$
    (c) Hard to find $H(H(m))$
    (d) Hard to find m given $H(m)$
    (e) None of the above

73. What type of forgery might you create given a hash function that has all security properties except second preimage resistance?
    (a) Selective
    (b) Perfect
    (c) Existential
    (d) Universal
    (e) None of the above

74. What type of forgery might you create given a hash function that has no collision resistance?
    (a) Selective
    (b) Perfect
    (c) Existential
    (d) Universal
    (e) None of the above

75. What type of forgery might you create given a hash function that always returns the first x bytes of m?
    (a) Selective
    (b) Perfect
    (c) Existential
    (d) Universal
    (e) None of the above

76. Which of the following is impossible for a hash function?
    (a) It never returns `10101` for any message
    (b) It returns `10101` for one message and `1010101` for another
    (c) It always returns the first x bytes of the message
    (d) It returns `10101` for one message and `10101` for another

(e) None of the above

77. All hash functions have which of the following properties?
    (a) Preimage resistance, second preimage resistance, collision resistance
    (b) Compression and extension
    (c) Compression and difficulty of computation
    (d) Compression and ease of computation
    (e) None of the above

78. All cryptographic hash functions have which of the following properties in addition to the properties of hash functions?
    (a) The ability use them to encrypt data
    (b) Preimage resistance, second preimage resistance, collision resistance
    (c) The ability to create inverse hashes
    (d) Extension and difficulty of reversal
    (e) None of the above

79. If $H(x) = f(g(x)||g(x))$ is collision resistant, which of the following must be true? Select the **most complete answer**.
    (a) g is collision resistant
    (b) Neither f nor g is necessarily collision resistant
    (c) f is collision resistant
    (d) Both f and g are collision resistant
    (e) None of the above

80. If we have $H(m)$ that always returns the first x bytes of m, how many of the three properties of cryptographic hash functions are broken?
    (a) 0
    (b) 1
    (c) 2
    (d) 3
    (e) None of the above

81. A function defined as $H(x) = 10101$ is a hash function.
    (a) True
    (b) False

82. A function defined as $H(x) = 10101$ is a cryptographic hash function.
    (a) True
    (b) False

83. A function defined as $H(x) = x$ is a hash function.
    (a) True
    (b) False

84. A function defined as $H(x) = x$ is a cryptographic hash function.

(a) True
(b) False

85. How many hashes do we need to store at any given time in the Rho method of finding collisions?
    (a) 2
    (b) 4
    (c) 20
    (d) 56
    (e) None of the above

86. What does a length extension attack allow us to do?
    (a) Create an existential forgery
    (b) Create the hash of a message that we do not explicitly know
    (c) Defeat MD5
    (d) All of the above
    (e) None of the above

87. What is the problem with Merkle-Damgard constructions?
    (a) They have limited compression
    (b) They are not really hash functions
    (c) They are susceptible to length extension attacks
    (d) They allow universal forgeries
    (e) None of the above

88. Which of the following is considered immune to length extension attacks?
    (a) SHA-1
    (b) SHA-2
    (c) SHA-3
    (d) All of the above
    (e) None of the above

89. Which of the following uses a sponge construction?
    (a) SHA-1
    (b) SHA-2
    (c) SHA-3
    (d) All of the above
    (e) None of the above

90. A MAC is which of the following?
    (a) A five-tuple (G, S, V, E, D)
    (b) A triple of efficient algorithms, (G, S, V)
    (c) A triple of efficient algorithms, (G, E, D)
    (d) A hash function without a key
    (e) None of the above

91. Which of the following is true about a CBC-MAC?
    (a) It has no compression property, unlike HMACs
    (b) It was invented by the CBC for tagging their broadcast data
    (c) It works by taking the entire ciphertext from a block cipher in CBC mode
    (d) It works by taking the last ciphertext block from a block cipher in CBC mode
    (e) None of the above

92. If you had a CBC-mode block cipher that produced `101 010 111 010 111 010` and it had a block length of 3 bits, what would be your CBC-MAC tag?
    (a) `010 111 010`
    (b) `101`
    (c) `101 010 111 010 111 010`
    (d) `010`
    (e) Not enough information

93. How does an EMAC work when the key for the original block cipher was k_1?
    (a) $E_{k_1}(c_\ell)$
    (b) $E_{k_2}(c_\ell)$
    (c) $E_{k_1}(E_{k_2}^{-1}(c_\ell))$
    (d) $E_{k_1}^{-1}(c_\ell)$
    (e) Either B or C
    (f) Either A or C

94. What makes an EMAC better than a CBC-MAC?
    (a) It adds extra security by adding diffusion
    (b) It allows arbitrary length messages
    (c) It has a faster runtime
    (d) It is actually worse because it is less efficient
    (e) None of the above

95. What is the preferred method of authenticated encryption?
    (a) Encrypt then MAC
    (b) Encrypt and MAC
    (c) Encrypt then hash
    (d) MAC then encrypt
    (e) None of the above

96. How does HMAC work?
    (a) $H\Big((k \oplus \text{opad}) || H\big((m \oplus \text{ipad})\big)\Big)$
    (b) $H\Big((m \oplus \text{opad}) || H\big((k \oplus \text{ipad})\big)\Big)$
    (c) $H\Big((k \oplus \text{opad}) || H\big((k \oplus \text{ipad}) || m\big)\Big)$
    (d) $H\Big((k \oplus \text{opad}) || H\big((k \oplus \text{ipad})\big) || m\Big)$

(e) None of the above

97. In an HMAC, the security is based on what?
    (a) The size of m
    (b) The underlying hash function used
    (c) The difference between opad and ipad
    (d) The number of times we run the algorithm
    (e) None of the above

For the next 5 questions, consider the following connection encrypted line from rbc.com:

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

98. What is the security protocol?
    (a) TLS 1.3
    (b) RSA
    (c) TLS ECDHE
    (d) TLS 1.2
    (e) None of the above

99. What block cipher is used to encrypt the message stream?
    (a) AES with 128 bit key and 256 bit block length
    (b) AES with 256 bit key and 256 bit block length
    (c) SHA with 384 bit block length and 256 bit key length
    (d) AES with 256 bit key and 128 bit block length
    (e) None of the above

100. What is the authentication scheme?
    (a) ElGamal public key encryption scheme
    (b) ElGamal signature scheme
    (c) RSA public key encryption scheme
    (d) RSA signature scheme
    (e) None of the above

101. What is the mode of operation for the block cipher?
    (a) GCM
    (b) CTR
    (c) CBC
    (d) ECB
    (e) None of the above

102. What is used to generate the MAC tag?
    (a) SHA-3 with 384 bit output
    (b) SHA-1 with 384 bit output
    (c) SHA-3 with 84 bit output
    (d) SHA-2 with 384 bit output
    (e) None of the above

103. What is a digital signature scheme?
    (a) Three-tuple (G, S, V)
    (b) Five-tuple (G, E, D, S, V)
    (c) Three-tuple (G, E, D)
    (d) A way or securely writing your name on a PDF
    (e) None of the above

104. In a DSS, the signing key is _____ and the verifying key is _____?
    (a) private, private
    (b) private, public
    (c) public, public
    (d) public, private
    (e) None of the above

105. Which of the following describes the generation algorithm in RSA DSS?
    (a) Take $N = pq$ and find e, d such that $ed = 1 \bmod \phi(N)$
    (b) Generate a random e, d
    (c) Take N as some large composite number and find e, d its prime factors
    (d) Generate a random N and take $e = \phi(N)$ and $d = N/e$
    (e) None of the above

106. Which of the following describes the signing algorithm in RSA DSS (assume public exponent is e and private is d)?
    (a) Compute $M = H(m)$ and $\sigma = M^d \bmod N$
    (b) Compute $M = H(m)$ and $\sigma = M^e \bmod N$
    (c) Compute $M = H(m)$ and $\sigma = M^d \bmod \phi(N)$
    (d) Compute $M = H(m)$ and $\sigma = M^e \bmod \phi(N)$
    (e) None of the above

107. Which of the following describes the verifying algorithm in RSA DSS?
    (a) Compute $M = H(m)$ and check if $\sigma^e \equiv M \bmod N$
    (b) Compute $M = H(m)$ and check if $\sigma^d \equiv M \bmod N$
    (c) Compute $M = H(m)$ and check if $\sigma^d \equiv M \bmod \phi(N)$
    (d) Compute $M = H(m)$ and check if $\sigma^e \equiv M \bmod \phi(N)$
    (e) None of the above

108. Which of the following is the secret key in ElGamal DSS?
    (a) x
    (b) g, x, p
    (c) g, x
    (d) g^x
    (e) None of the above

109. Which of the following is the public key in ElGamal DSS?
    (a) g, g^x, p
    (b) g, p

(c) x
(d) g, x, p
(e) None of the above

110. How do you verify a signature in ElGamal DSS?
(a) Check if $H(m)^g = (g^x)^r r^s \bmod p$
(b) Check if $g^{H(m)} = xr^s \bmod p$
(c) Check if $g^{H(m)} = (g^x)^r r^s \bmod p$
(d) Check if $g^{H(m)} = x^r r^s \bmod p$
(e) None of the above

111. The security of the ElGamal signature scheme relies on which of the following?
(a) Computational DH
(b) Decisional DH
(c) Factoring large numbers mod p
(d) Discrete log problem
(e) None of the above

112. What is g in the ElGamal signature scheme?
(a) A generator in $\mathbb{Z}_p^*$
(b) A large prime number
(c) A random base
(d) A random exponent
(e) None of the above

113. How many copies of keys are needed for n parties to communicate with each other using secret key crypto without a PKI?
(a) $O(n^2)$
(b) $O(n \log_2 n)$
(c) $O(n)$
(d) $O(\log_2 n)$
(e) None of the above

114. How many copies of keys are needed for n parties to communicate with each other using public key crypto without a PKI?
(a) $O(n^2)$
(b) $O(n \log_2 n)$
(c) $O(n)$
(d) $O(\log_2 n)$
(e) None of the above

115. What does a PKI do?
(a) Allows you to quickly share secret keys
(b) Allows you to check which public key belongs to whom
(c) Allows you to quickly generate public keys
(d) Allows you to communicate securely without cryptography

(e) None of the above

116. Which of the following is **not** an example of a PKI?
    (a) WoT
    (b) sPKI
    (c) CA
    (d) TLS
    (e) All of the above **are** examples of PKIs

117. CAs are generally presented as a hierarchy.
    (a) True
    (b) False

118. Self-signing a certificate at the top level of a hierarchy is generally good practice.
    (a) True
    (b) False

119. In a web of trust, you generally sign your own keys.
    (a) True
    (b) False

120. In a web of trust, other users generally sign your keys.
    (a) True
    (b) False

121. How many signatures do you need to trust to accept a key in a web of trust?
    (a) At least 1
    (b) None
    (c) At least $n^2/2$ where n is the number of WoT members
    (d) At least $n/2$ where n is the number of WoT members
    (e) None of the above

122. In a $(4, 8)$ secret sharing scheme, how many shares do we need to fully reconstruct the secret?
    (a) 8
    (b) 2
    (c) 24
    (d) 4
    (e) None of the above

123. What is one caveat of Threshold ElGamal?
    (a) It allows existential forgeries of the secret shares
    (b) It requires a trusted third party
    (c) It has no caveats
    (d) It is much slower than Shamir Secret Sharing for high thresholds
    (e) None of the above

124. Which of the following does Shamir Secret Sharing rely on?
    (a) The difficulty of factoring the modulus
    (b) A trusted third party
    (c) Lagrange interpolation at $f(1)$
    (d) Lagrange interpolation at $f(0)$
    (e) None of the above

125. What is completeness in a zero knowledge proof?
    (a) The verifier will learn the prover's knowledge
    (b) The prover will not convince the verifier if they are not telling the truth
    (c) The prover will convince the verifier if they are telling the truth
    (d) The verifier does not learn anything about the prover's knowledge
    (e) None of the above

126. What is soundness in a zero knowledge proof?
    (a) The verifier will learn the prover's knowledge
    (b) The prover will not convince the verifier if they are not telling the truth
    (c) The prover will convince the verifier if they are telling the truth
    (d) The verifier does not learn anything about the prover's knowledge
    (e) None of the above

127. What is zero-knowledgeness in a zero knowledge proof?
    (a) The verifier will learn the prover's knowledge
    (b) The prover will not convince the verifier if they are not telling the truth
    (c) The prover will convince the verifier if they are telling the truth
    (d) The verifier does not learn anything about the prover's knowledge
    (e) None of the above

128. What is the binding property in a commitment scheme?
    (a) The statement should remain revealed until the user hides it
    (b) The statement should remain hidden until the user reveals it
    (c) When a user commits to a statement, they cannot change it
    (d) A user cannot change whom they are communicating with after committing to it
    (e) None of the above

129. What is the hiding property in a commitment scheme?
    (a) The statement should remain revealed until the user hides it
    (b) The statement should remain hidden until the user reveals it
    (c) When a user commits to a statement, they cannot change it
    (d) A user cannot change whom they are communicating with after committing to it
    (e) None of the above

130. A commitment scheme can be build with cryptographic hash functions.
    (a) True
    (b) False