Name _____

Test 1 for CS 591 V1: Applied Crypto

You must complete this test alone, without using any written references or a calculator. Write your name on each page. Respond clearly and legibly to all questions.

This test contains **39** questions worth a total of **100** points. For the first section on terminology, each of the 40 blanks is worth 1 point each. The subsequent 15 short answer questions are worth 4 points each.

If your answer doesn't fit in the provided space, use the "extra space" section at the end of the test. Within the question itself, make sure to provide a clear pointer that your response is continued in the extra space section.

Terminology (40 points, 1 point per blank)

Complete the sentences below about the crypto concepts we learned in class. Some questions have more than one blank and are thus are worth multiple points. Some blanks have multiple valid answers; any one will suffice.

Block ciphers

1. The field of cryptology is split into cryptography (for defense) and _____ (for offense).

2. The most popular block cipher in use today is _____ .

3. The 4 subroutines called repeatedly within the most popular block cipher are: _____ , _____, _____, and _____ .

4. I stated in class that a block cipher must satisfy three design goals: it must be simple, it must make no sense, and _____ .

5. We formally codify the "makes no sense" goal of a block cipher with the notion of _____ .

6. We design block ciphers as an iterative series of _____ that each only make partial sense.

7. List Claude Shannon's 2 security goals for a block cipher: _____ and _____ .

8. In a tweakable block cipher, the key provides secrecy whereas the tweak provides _____ .

Message authentication codes

9. The most popular message authentication code in use today is _____ .

10. The security guarantee we want MACs to achieve is _____ (write out full words here), which we often abbreviate with the acronym _____ .

11. With a MAC, the recipient of a message can _____ the sender and also guarantee that the message has not been _____ from its original form in transit.

12. A MAC does not prevent Mallory from performing a _____ attack. A higher-level protocol needs to handle this, say by using nonces or timestamps to guarantee uniqueness.

13. Explain why ECB mode isn't a good MAC, even when restricted only to messages that are exactly 2 blocks in length: _____ .

Symmetric key encryption schemes

14. The most popular encryption mode of operation in use today is_____ .

15. The minimal security guarantee we want encryption to achieve is _____ (write out full words here), which we often abbreviate with the acronym _____ .

16. The initialization vector in CBC mode must be _____ for the encryption scheme to be secure. The initialization vector in CTR mode must satisfy a different guarantee:_____ .

17. Of the two popular encryption modes: _____ mode doesn't need padding. _____ mode does need padding unless you use _____(this technique is also used in disk encryption).

18. Explain why ECB mode isn't a good encryption scheme, even when restricted only to messages that are exactly 2 blocks in length: _____ .

Hash functions

19. The most popular hash function in use today is _____ .

20. Complete Katz and Lindell's explanation of why a truly random function *R* is a worthwhile ideal goal against which to compare real cryptosystems. "If an adversary A has not_____ on some input x, then the value of *R*(x) is _____ …at least as far as A is concerned."

21. For any hash function H: $\{0,1\}^* \rightarrow \{0,1\}^n$, the_____attack chooses inputs at random and records outputs until a collision is found. It requires about _____invocations of *H* to find a collision.

22. The Merkle-Damgard construction builds a hash function using a _____ as a building block. By contrast, the sponge function construction starts with a _____ instead.

23. The state of a sponge function is split into two pieces: the _____ that affects performance and the _____ that affects security.

24. Order the following 3 security notions for hash functions from easiest to hardest *to break*: collision resistance, preimage resistance, and second preimage resistance.
_____, _____, and _____
(easiest to break, so hardest to achieve) (middle) (hardest to break)

Name _____

Formal definitions (24 points total, 4 points each)

For each of the two cryptographic primitives listed in bold below, answer the following questions.

Message authentication codes

25. List the 3 algorithms that comprise a MAC. Clearly mark all inputs and outputs.

26. Describe the security guarantee that MACs achieve. You may draw pictures, but you should not *only* draw pictures; also to explain in words what powers Mallory possesses and what she still cannot do.

27. Explain why a MAC doesn't necessarily provide any privacy guarantees.

Symmetric key encryption schemes

28. List the 3 algorithms that comprise an encryption scheme. Clearly mark all inputs and outputs.

29. Describe the security guarantee that symmetric encryption achieves. You may draw pictures, but you should not *only* draw pictures; also to explain in words what powers Mallory possesses and what she still cannot do.

30. Explain why an encryption scheme doesn't necessarily provide any integrity guarantees.

Name _____

Length extension attacks (24 points total, 4 points each)

For each of the two constructions listed in bold below, answer the following questions.

The CBC-MAC message authentication code

31. Draw a diagram showing how CBC-MAC works. Clearly state any cryptographic primitives required.

32. Show concretely how CBC-MAC is vulnerable to a length extension attack.

33. Describe *two* distinct changes to CBC-MAC that eliminate the threat of length extension.

The Merkle-Damgard construction of hash functions

34. Draw a diagram showing how Merkle-Damgard works. Clearly state any cryptographic primitives required.

35. Show concretely how Merkle-Damgard is vulnerable to a length extension attack.

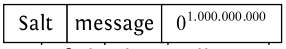
36. Describe *two* distinct changes to Merkle-Damgard that eliminate the threat of length extension.

Name _____

Constructions (12 points total, 4 points each)

37. We call the hash functions MD5 or SHA-1 *broken* whereas we call the block cipher DES *obsolete*. Why do we use different terms when describing our views of these objects?

38. Explain why it is the case that for messages that are exactly 1 block in length, calling the block cipher alone suffices as a message authentication code. (You don't need to provide a formal reduction here; simply explain the intuition behind the idea in writing.)

39. When building a hash function for passwords using a sponge function design, absorption occurs in the following order: 

(this figure is taken directly from the Keccak team's slides). Explain the purpose of the long all-zeros string and also explain why the 3 inputs are absorbed in this order.

Extra space

If you need additional space to respond to any question, continue your answer here. You may also use the back of this page if needed. Make sure that you write the number of the question that you're answering.