Name _____

Exam for CS 591 V1: Applied Crypto

This test contains **35** questions worth a total of **200** points. The value of each question is clearly marked.

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

Terminology (60 points)

(3 points each) State the concept that the sentence describes. Each response should be only a few words. Some questions have multiple correct responses; if you write any one of them, you will receive full credit.

1. The field of _____ is split into two pieces: the science of making "unbreakable" codes, denoted _____, and the science of breaking codes, denoted_____ .
2. The winner of the Advanced Encryption Standard (AES) competition was the cipher_____ .
3. The _____ attack on dual-DES (2DES) is one example of a time-memory tradeoff.
4. The _____ of a block cipher or hash function is defined as the number of rounds in the primitive minus the number of rounds we know how to break.
5. In a tweakable block cipher, the key provides secrecy and the tweak provides _____ .
6. Auguste Kerckhoffs' principles for cipher design include the statement that _____ _____ so that Alice and Bob have the ability to recover from a previous compromise.
7. NIST's SHA-3 competition evaluated submissions by "The extent to which the [proposed] algorithm output is indistinguishable from a_____." (This is an "ideal" hash function.)
8. Common unit of measurement for speed of cryptosystems in software: _____ per _____ .
9. If Alice protects her messages with this primitive before transmitting it to Bob, then Mallory will effectively not be able to *learn* anything about their contents: _____ .
10. If Alice protects her messages with this primitive before transmitting it to Bob, then Mallory will effectively not be able to *alter* their contents: _____ .
11. This primitive simultaneously provides both privacy and integrity, thereby encompassing the guarantees of the prior 2 questions: _____ .
12. Most common mode of operation used to instantiate the combined primitive: _____ .
13. Give one reason why the mode in question #13 is popular: _____ .
14. This technique eliminates the need to pad messages in CBC mode: _____ .
15. This performance optimization computes a cipher on multiple inputs simultaneously: _____ .
16. Best mode of operation for key wrapping, which protects one crypto key under another: _____ .
17. A _____ attack simply tries all possible keys in order, and tests which one works.
18. A _____ attack simply picks inputs at random until it finds two that collide.
19. Following up on question #18: if we draw items with replacement from a set of size *L*, then the expected number of items to draw before the first collision is approximately _____ .
20. The term _____ encapsulates all potential sources of info about a cryptosystem that leak out due to its implementation, but which fall outside of our mathematical definitions.

Name _____

Security guarantees (40 points)

21. (12 pts) Name and define (in words, math, or pictures) the security guarantee that block ciphers meet.

22. (12 pts) Briefly define Claude Shannon's two security goals for block ciphers. Then explain why block ciphers need each one (i.e., why the security guarantee in the previous question fails without it).

Goal	What it is	Why block ciphers need it
Confusion		
Diffusion		

23. (12 pts) Describe the following security notions. For each guarantee, state the powers that we provide to Mallory to facilitate a potential attack, and explain the thing Mallory cannot do anyway.

Definition	Mallory's capabilities	What Mallory still cannot do
IND$-CPA		
EU-CMA		

24. (4 pts) This question considers the relative strength of the following three security notions for hash functions: collision resistance, preimage resistance, and second preimage resistance.

    - Which provides the strongest security guarantee for the defender (or in other words, is the easiest for the attacker to break)? _____
    - Which provides the weakest security guarantee for the defender (or in other words, is the hardest for the attacker to break)? _____

Name _____

Constructions (40 points)

25. (16 pts) Summarize the operation of and security benefits provided by each component within AES.
    - SubBytes:
    - ShiftRows:
    - MixColumns:
    - AddRoundKey:

26. (8 pts) Describe a concrete scenario in which the following events hold. Explain your rationale.
    - CTR mode is better than CBC:
    - CBC mode is better than CTR:

27. (8 pts) Draw a picture depicting the Merkle-Damgard construction. What building block does it use?

28. (8 pts) Draw a picture depicting the sponge function construction. What building block does it use?

Name _____

Attacks (30 points)

29. (30 pts) Describe the following three attacks on implementations of cryptosystems. Explain the *problem* the attack exploits and state *how* the attack exploits this problem to extract the key.

Attack	Problem it exploits	How the attack works
Padding oracle		
Cache timing		
Power analysis		

Protecting passwords (30 points)

The remaining questions pertain to the 2013 data breach of 38 million users' password data from Adobe Systems, Inc. I'll briefly summarize what happened. Somebody hacked into Adobe's servers and exfiltrated a large (~10 GB) database containing user data. Each record within the leaked database includes a username and some base-64 encoded data pertaining to the user's password. Adobe quickly sent its customers a security alert stating that "attackers may have obtained access to your Adobe ID and encrypted password." The most surprising word here is *encrypted*.

At first, it was assumed that Adobe's public announcement was simply using the word 'encrypted' in a non-technical, intuitive manner since that word is better understood by the general public than the word 'hashed.' However, upon further investigation, researchers found out that Adobe was in fact telling the truth! The following picture shows a few randomly-chosen rows of the password database in hex.

Password data (hex)	Password hint
0b4c27d8f75cc41a	-> Same old, same old
e826ef87cc7a3029 e2a311ba09ab4707	-> You'll never guess
0842ccb7edf3e343 e2a311ba09ab4707	->
92663700893c3f27 a667d747891a8255	-> Dog + digit
88fc540356d561ec	-> Dog
fb0a9047a5dd5ef8 f3c512b0e38a5392 a3f492fbd917f632	-> Virtuously long
92bb535704f0ae7f	-> Geburtestag

Note that different encrypted passwords have different lengths, and each is a multiple of 8 bytes; this provides evidence that the passwords are in fact *encrypted*, not hashed. Furthermore, the 8 byte block size leads researchers to believe that the block cipher involved is likely DES or Triple-DES (3DES); it's definitely not AES, since that has a 16 byte block size. Additionally, ciphertexts repeat throughout the database, which indicates that the encryption likely uses ECB mode.

This is a fantastically terrible design for password storage! In the following questions, you will explain precisely *why* Adobe's design was so bad.

More precisely: the six questions in this section ask you to explain the distinction (from a security point of view) between two proposed protection mechanisms that Adobe could have implemented. Describe an explicit attack that is possible (or made much easier) against the weaker setup but not the stronger one.

30. (5 pts) Hashing passwords using the password-based hash function PBKDF2 versus the 'ordinary' hash function SHA-256, where both are salted uniquely for each user and have the salt stored in the clear.

31. (5 pts) Hashing passwords with SHA-256 that's salted uniquely for each user versus unsalted SHA-256.

32. (5 pts) Hashing passwords with SHA-256 versus encrypting them using AES with any mode of operation that achieves IND$-CPA (such as CBC or CTR modes).

33. (5 pts) Encrypting passwords with a semantically secure mode versus with ECB mode.

34. (5 pts) Encrypting passwords using AES versus 3DES, both using ECB mode.

35. (5 pts) Encrypting passwords using 3DES versus DES, again both using ECB mode.

Name _____

Extra space

If you need additional space to respond to any question, continue your answer here. Make sure that you write the number of the question that you're answering.