Name _____

Final Exam for CS 591 V1: Applied Crypto

You must complete this test alone, without using any written references or a calculator. Respond clearly and legibly to all questions. Feel free to add diagrams if you think they will help. **Write your name on each page.**

This test contains 70 questions worth a total of 300 points. For each short question, provide a 1-sentence answer for 4 points. Longer form responses are worth 6 points. The final section on Comparisons has a different rubric.

Terminology (68 points)

Data protection: Define the 4 types of data protection we want when Alice attempts to send a message to Bob.

1. Binding: _____
2. Confidentiality: _____
3. Deniability: _____
4. Identity verification: _____

Principles of cipher design: Explain the properties that each person stated that block ciphers should satisfy.

5. Auguste Kirckhoffs: _____
6. Claude Shannon: _____

Cipher terminology: Define these terms that relate to block ciphers or hash functions.

7. Rounds: _____
8. Brute force attack: _____
9. Random oracle: _____

AES round function components: Explain the security benefits that each operation provides toward AES.

10. SubBytes:_____
11. ShiftRows: _____
12. MixColumns: _____
13. AddRoundKey:_____

Modifications: Explain how the italicized adjective enhances the performance or security of its base primitive.

14. *Tweakable* block cipher: _____

15. *Salted* hash function: _____

16. *Password-based* hash function: _____

17. CBC mode *with ciphertext stealing*: _____

Constructions (56 points)

18. The SHA-2 hash function follows a _____ design. (It's like a mode of operation.) By contrast, SHA-3 uses a _____ design.

19. When combining an encryption scheme and a MAC in a generic fashion, explain why Enc-then-MAC is preferable to MAC-then-Enc. Make sure your explanation clearly states a specific concern with the latter.

20. Suppose Alice and Bob have never communicated before. Explain how they can use the *Diffie-Hellman key exchange protocol* to derive a shared symmetric key while only sending non-sensitive communications.

21. Suppose Alice and Bob have already negotiated a shared symmetric key K. Explain 1 method they can use for *key evolution* to a new key K' that (a) only uses symmetric crypto primitives and (b) provides forward secrecy.

22. Describe 1 specific coding convention that you *should* follow when implementing a cryptographic system but that you *should not* follow otherwise (i.e., that ordinarily would be considered a poor programming practice).

Name _____

Properties of (auth) encryption modes: Each statement below applies to exactly 1 or 2 of the following modes of operation: CBC, CTR, XTS, CCM, EAX, GCM, and SIV. List the mode or modes that satisfy the listed property.

23. Good for key wrapping (that is, encrypting one key under another one): _____

24. Used for full disk encryption of data stored in laptops and smartphones: _____

25. Popular for protecting data in transit on the internet due to Intel hardware acceleration: _____

26. Requires two separate passes through the data: _____

27. Authenticated encryption mode designed to be streaming-friendly: _____

28. Confidentiality is *not* achieved via a counter mode design: _____

Security definitions (18 points)

29. Using words and/or pictures, explain the concept of *pseudorandomness* that block ciphers must achieve.

30. Using words and/or pictures, explain the following security notions for hash functions: *preimage resistance*, *second preimage resistance*, and *collision resistance*. Which is the hardest security notion to achieve?

31. Using words and/or pictures, explain the concepts of *forward secrecy* and *backward secrecy*.

The Signal protocol (24 points)

Properties of Signal: Explain which portion of the construction of Signal yields the following security properties.

32. Deniability: _____

33. Forward secrecy: _____

34. Backward secrecy: _____

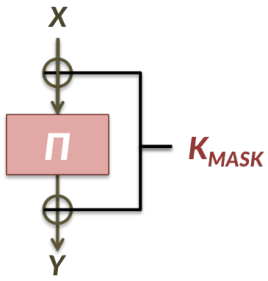
Operation of Signal: Suppose Alice wishes to initiate a chat with Bob for the first time. Explain the process below.

35. What information must Bob have provided to the Signal server beforehand? How does Alice use this info?

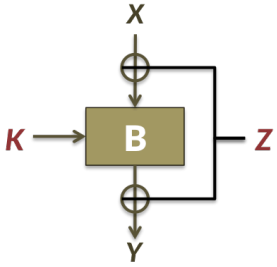
36. Keys in Signal are derived via a *triple Diffie-Hellman protocol*, which combines the information Alice gains in the prior question with a long-term key for each of Alice and Bob. Since Signal strives to provide deniability, then why does it include any long-term state? Also, how is Signal able to achieve deniability anyway?

Attacks on constructions (42 points)

37. The Even-Mansour construction is proved to yield a block cipher when instantiated with a public, truly random permutation *Π.* In this question, please show that the construction is *minimal*, in the sense that removing the permutation or either one of the xor operations results in a construction that is no longer pseudorandom.

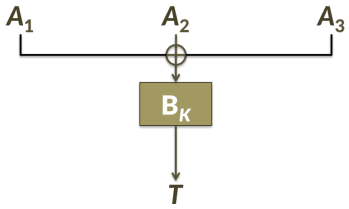


38. Show that the modified Even-Mansour construction on the right is *not* a tweakable block cipher. In this construction, B denotes a block cipher with key K, and the pre- and post-xors now apply the tweak Z.



Name _____

39. Let B_K be a block cipher, and consider the following XOR-based construction of a message authentication code. Show how to break this MAC.



40. The hash function MD5 is vulnerable to a *chosen-prefix attack* whereas the hash function SHA-1 is vulnerable to an *identical-prefix attack*. Please explain the difference between these two attacks.

41. This question considers the *meet in the middle* attack on 2 instances of a block cipher (like 2DES). Please explain how to conduct this attack, and also state the running time and space required to conduct it.

42. You observe the 5 ECB mode-created plaintext/ciphertext pairs, and you know the underlying block cipher used has a block size of 3 characters. Use this information to decrypt 3 ciphertexts: `abc123`, `mnovwx`, `yz0jkl`.

Input	Output
canine	abcdef
gender	ghijkl
mishap	mnopqr
rescue	stuvwx
saddle	yz0123

43. Consider the 3-bit S-box defined by the truth table on the right. Calculate the probability that an input difference Δx = 1 translates to an output difference Δy = 2. (Remember that 'difference' here means xor.)

x	0	1	2	3	4	5	6	7
y	6	4	3	1	5	0	2	7

Name _____

Comparisons (92 points)

This section asks several questions about the properties provided by, or required of, the constructions and attacks we studied in class. You must answer each question on the left for every construction or attack mentioned. For questions that seek a 'yes' or 'no' response, please circle the correct answer. Some of the questions require free-form text answers. In this section, yes/no questions are worth 1 point and free text boxes are worth 2 points each.

Comparing MACs (8 points): Indicate if the following statements are true for CBC-MAC and HMAC.

	CBC-MAC	HMAC
44. Uses an initialization vector (IV)?	Yes / No	Yes / No
45. Safe to use also as a hash function?	Yes / No	Yes / No
46. We have a security reduction to the pseudorandomness of its underlying cipher or compression function?	Yes / No	Yes / No
47. Vulnerable to a length extension attack (assuming that recipient doesn't know the input length in advance)?	Yes / No	Yes / No

Comparing encryption modes (26 pts): Indicate whether the following statements hold for CBC and CTR modes.

	CBC mode	CTR mode
48. Broken if its initialization vector (IV) is predictable?	Yes / No	Yes / No
49. Broken if IV is reused?	Yes / No	Yes / No
50. Its ciphertexts are malleable by Mallory?	Yes / No	Yes / No
51. Natively requires padding to the block length?	Yes / No	Yes / No
52. Decryption requires the use of decipher routine B_K^{-1}?	Yes / No	Yes / No
53. If network mistakenly *drops* 2nd block of ciphertext…		
a. 1st block of plaintext is unrecoverable	Yes / No	Yes / No
b. 2nd block of plaintext is unrecoverable	Yes / No	Yes / No
c. 3rd block of plaintext is unrecoverable	Yes / No	Yes / No
d. All future blocks of plaintext are unrecoverable	Yes / No	Yes / No
54. If network mistakenly *corrupts* the 2nd block of ciphertext (i.e., transmits a different block instead)…		
a. 1st block of plaintext is unrecoverable	Yes / No	Yes / No
b. 2nd block of plaintext is unrecoverable	Yes / No	Yes / No
c. 3rd block of plaintext is unrecoverable	Yes / No	Yes / No
d. All future blocks of plaintext are unrecoverable	Yes / No	Yes / No

Comparing security notions (18 points): Indicate whether the fundamental security guarantees for MACs, hashes, and encryption schemes require that *all* compliant constructions achieve the properties listed on the left.

	EU-CMA for message authentication codes	Collision resistance for hash functions	IND$-CPA for encryption schemes
55. Requires a key?	Yes / No	Yes / No	Yes / No
56. Must be deterministic?	Yes / No	Yes / No	Yes / No
57. Must be randomized?	Yes / No	Yes / No	Yes / No
58. Output length ≥ bits of security?	Yes / No	Yes / No	Yes / No
59. Always length increasing? (Output length > input length)	Yes / No	Yes / No	Yes / No
60. Always length decreasing? (Output length < input length)	Yes / No	Yes / No	Yes / No

Name _____

Comparing hash functions (12 pts): Indicate if the following statements hold for SHA-2 and SHA-3 (aka Keccak).

	SHA-2	SHA-3
61. Susceptible to length extension attacks?	Yes / No	Yes / No
62. Susceptible to birthday bound attacks?	Yes / No	Yes / No
63. Supports variable output lengths?	Yes / No	Yes / No
64. Can build a MAC from it using the HMAC construction?	Yes / No	Yes / No
65. Nevertheless, shouldn't build a MAC from it via HMAC?	Yes / No	Yes / No
66. Significant usage today in TLS to protect web traffic?	Yes / No	Yes / No

Comparing side-channel attacks (28 points): Describe how these attacks operate from the attacker's perspective.

	Padding oracle	Timing	Cache timing	Power analysis
67. Attacker is passive Eve or active Mallory?	Passive / Active	Passive / Active	Passive / Active	Passive / Active
68. What type of data do you collect about the world? That is, what is the physical measurement that you make?				
69. What does this observation reveal about the ciphertext? That is, what property of the underlying plaintext have the attackers *leaked* to you?				
70. How does this leakage relate to the secret key? That is, how can you find the key with enough of the leaked information?				

Name _____

Extra space

If you need additional space to respond to any question, continue your answer on this page. Make sure to write here the number of the question that you're answering. Also, within the question itself, provide a clear pointer that your response is continued in the extra space section.