Name _____ BU ID # _____

Midterm for CS 568: Applied Cryptography

This test contains 40 questions worth a total of 100 points. You must complete the test alone, without using any written references or a calculator. Respond clearly and legibly to all questions. ***Write your name on each page.***

Multiple choice questions (2 points each, 60 points total)

For all of the following questions, fill in the bubble to the ***left*** of your desired answer(s). Questions might have multiple correct answers. To get full credit, you must mark all correct answers and no incorrect ones.

Principles of cipher design

Match each person's name with an important cryptographic principle that they advocated.

1. Anyone can build a cipher that looks unbreakable to them .... ☐ A. Kerckhoffs ☐ B. Schneier ☐ C. Shannon
2. Ciphers should be confusing and diffusing ..... ☐ A. Kerckhoffs ☐ B. Schneier ☐ C. Shannon
3. The only secret in a cipher should be an easily-changed key .. ☐ A. Kerckhoffs ☐ B. Schneier ☐ C. Shannon

Cryptographic building blocks

Mark whether each property applies to block ciphers or hash functions. *Remember: both are possible!*

4. Requires a secret key ..... ☐ Block cipher ☐ Hash function
5. Can build from a compression function by the Merkle-Damgard paradigm .. ☐ Block cipher ☐ Hash function
6. Can use to build a message authentication code (MAC) ..... ☐ Block cipher ☐ Hash function
7. SHA2 is the most popular instantiation of this ..... ☐ Block cipher ☐ Hash function
8. Is efficiently invertible ..... ☐ Block cipher ☐ Hash function
9. A mode of operation is built from many applications of this ..... ☐ Block cipher ☐ Hash function
10. Can be broken via a birthday attack ..... ☐ Block cipher ☐ Hash function

Cryptographic systems to protect data at rest

Mark whether encryption schemes or message authentication codes provide each objective.

11. Provides message privacy: the attacker cannot learn any part of the message ..... ☐ Encryption ☐ MAC
12. Provides authenticity: Alice knows she created the message & can detect tampering .. ☐ Encryption ☐ MAC
13. Strong enough to withstand an actively malicious Mallory, not just passive Eve ..... ☐ Encryption ☐ MAC
14. Used to protect hard drives sector-by-sector, when there is no extra space on disk ..... ☐ Encryption ☐ MAC

MACs for long messages

For each property stated, mark all of the MACs for which the property holds. (Reminder: CMAC == XMAC.)

Name _____ BU ID # _____

15. Constructed from a hash function (rather than a block cipher) .. ☐ CBC-MAC ☐ CMAC ☐ OMAC ☐ HMAC

16. Requires Alice to remember multiple keys ..... ☐ CBC-MAC ☐ CMAC ☐ OMAC ☐ HMAC

17. Vulnerable to a length extension attack ..... ☐ CBC-MAC ☐ CMAC ☐ OMAC ☐ HMAC

18. Would be broken if used as a cryptographic hash function ..... ☐ CBC-MAC ☐ CMAC ☐ OMAC ☐ HMAC

Security definitions for encryption
Mark whether each property is achieved by indistinguishability (IND) or pseudorandomness (IND$) under CPA.

19. Defined via a challenge game played between Alice and the attacker ..... ☐ IND-CPA ☐ IND$-CPA

20. The stronger of the two definitions, and thus more desirable for Alice ..... ☐ IND-CPA ☐ IND$-CPA

21. CBC and CTR modes achieve it, potentially against nonce-respecting attackers ..... ☐ IND-CPA ☐ IND$-CPA

Additional multiple choice questions
Answer the following questions. Remember that more than one answer may be correct.

22. The winner of the AES block cipher competition ..... ☐ MARS ☐ RC6 ☐ Rijndael ☐ Serpent ☐ Twofish

23. Acceptable block lengths for AES ..... ☐ 56 bits ☐ 112 bits ☐ 128 bits ☐ 192 bits ☐ 256 bits

24. Acceptable key lengths for AES ..... ☐ 56 bits ☐ 112 bits ☐ 128 bits ☐ 192 bits ☐ 256 bits

25. The S-box of a block cipher is ..... ☐ Applied independently to different parts of the state ☐ Non-linear

26. In a tweakable block cipher, the tweak provides ..... ☐ Agility ☐ Secrecy ☐ Variety

27. What is ciphertext stealing used for? ... ☐ Attacking encryption ☐ Avoiding padding ☐ Meet-in-the-middle

28. When booting an encrypted phone, how does it get the key? ..... ☐ Derive from pin ☐ Read from RAM

29. While using an unlocked encrypted phone, how does it get the key? .. ☐ Derive from pin ☐ Read from RAM

30. DES has a 56 bit key and 3DES has a 112 bit key. In the time that it would take to do one 3DES brute force attack, how many DES brute force attacks could you do instead? ..... ☐ 2 ☐ 56 ☐ 2^{56}

Free form questions (4 points each, 40 points total)

For each question, please explain the stated security definitions, cryptographic constructions, or attacks. Each answer will require a few sentences; additionally, feel free to draw any diagrams as you see fit. If you need additional space to respond to any question, continue your answer in the "Extra space" section at the end of the test, and ***provide a clear pointer*** that your response is continued in the extra space section!

Name _____ BU ID # _____

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

32. Suppose the block cipher *B* is strongly pseudorandom. Let *B'* be a new block cipher with double the block and key length that operates as follows: its key generation chooses two independent keys *K1* and *K2*, and its encipher routine $B'_{K1,K2}(X_1, X_2) = B_{K1}(X_1) \,||\, B_{K2}(X_2)$ feeds the two halves of its block into 2 independent instances of *B* with different keys. (Decipher works similarly.) Question: is *B'* pseudorandom? Why or why not?

33. You observe the following plaintext/ciphertext pairs that Alice "encrypted" using ECB mode with a block cipher whose block length is 3 characters. Using this information, decrypt the ciphertexts `defmno` and `pqrghi`.

Plaintext	Ciphertext
`advice`	`abcdef`
`eerily`	`ghijkl`
`boxcar`	`mnopqr`

34. Write the name of the security definition for MACs that we abbreviate as EU-CMA. Then, explain it in words or diagrams. Describe clearly the capabilities provided to the attacker and what she still cannot do.

35. Explain why applying SHA2 to Alice's secret key *K* and message *A* does not suffice as a MAC. Concretely, if Alice constructs tag *T* = SHA2 (*K* || *A*), then show how Mallory can break EU-CMA. (Here, || denotes concatenation)

36. Explain why a MAC is susceptible to replay attacks even if it satisfies EU-CMA. Recall that in a replay attack, Mallory reverts Alice's hard drive to an old version that contains messages and tags that Alice made previously. Your response to this question should explain why EU-CMA doesn't forbid replay attacks from happening.

37. For each security notion for a hash function *H*, state the information Mallory is given and what she must find.

Security notion	*What Mallory is given*	*What she must find*
Preimage resistance		
Second preimage resistance		
Collision resistance		

38. Explain one security definition for encryption systems, either IND-CPA or IND$-CPA (circle which option you choose). Describe clearly the capabilities provided to the attacker and what she still cannot do.

Name _____ BU ID # _____

39. CBC mode has 2 differences from CBC-MAC. In this question, you must show why those changes are necessary.

    a. Explain why CBC would be a bad encryption scheme if we *did not* xor the first block of message with an initialization vector (IV) — or equivalently, if the IV were always set equal to 0.

    b. Explain why CBC would be a bad encryption scheme if we *only* output the final block of data.

40. CBC-MAC has 2 differences from CBC. In this question, you must show why those changes are necessary.

    a. Explain why CBC-MAC would be a bad message authentication code if we *did* have an IV.
    (Note that the IV would need to be part of the tag so that future Alice can use it when verifying.)
    [to fix: does the attacker control the IV?]

    b. Explain why CBC-MAC would be a bad message authentication code if we output *all* blocks of data.

Extra credit (5 points)

41. Suppose your friend comes to you and says "I designed a new encryption scheme that I believe is strong and everyone should use." How would you respond to your friend? (Note: there are many valid answers to this question. We will accept any answer as long as you justify it; do not simply write a one-word yes/no answer.)

Name _____ BU ID # _____

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 statement*** that we should look for the rest of your answer in the extra space section.