Name _____ BU ID # _____

Final Exam for CS 568: Applied Cryptography, Spring 2019

This test contains 60 questions worth a total of 100 points. You must complete the test alone, without using any written or electronic aids. Respond clearly and legibly to all questions. ***Write your name and BU ID on each page.***

Single choice questions (25 questions worth 1 point each, 25 points total)

For each question below, fill in the bubble to the ***left*** of your response. Each question has exactly 1 correct answer.

Shannon's properties of block ciphers

Mark whether the stated property applies to confusion or diffusion. Exactly one answer is correct.

1. Ensures uncertainty of any row of the truth table, as long as the key is unknown .... O Confusion O Diffusion
2. Ensures uncertainty between rows of the truth table, with an unknown key ..... O Confusion O Diffusion
3. The ideal version of this property is when the cipher *avalanches* ..... O Confusion O Diffusion
4. Within a block cipher, a substitution box primarily provides this ..... O Confusion O Diffusion
5. Within a block cipher, a linear permutation primarily provides this ..... O Confusion O Diffusion

Cipher block chaining modes

For each property stated, mark whether it applies to CBC encryption or CBC-MAC. Exactly one answer is correct.

6. Guaranteed that output length ≥ input length ..... O CBC O CBC-MAC
7. Safe to apply padding on messages that are not a multiple of the block length ..... O CBC O CBC-MAC
8. Is deterministic ..... O CBC O CBC-MAC

Key agreement protocols

Mark the cryptographic protocol(s) for agreeing on a shared symmetric key that apply to each statement.

9. Only uses symmetric cryptography ..... O Diffie-Hellman O Needham-Schroeder
10. Used within the Signal protocol ..... O Diffie-Hellman O Needham-Schroeder
11. Server connecting Alice and Bob will learn the shared key ..... O Diffie-Hellman O Needham-Schroeder

Applicability of cryptographic constructions

Mark whether each cryptosystem protects data at rest, in transit, or in use. Exactly one answer is correct.

12. Oblivious pseudorandom function ..... O Protects at rest O Protects in transit O Protects in use
13. Signal protocol ..... O Protects at rest O Protects in transit O Protects in use
14. XTS mode ..... O Protects at rest O Protects in transit O Protects in use

Name _____ BU ID # _____

Protecting data in transit against the threat of device compromise
Mark whether each statement applies to forward or backward secrecy. Exactly one answer is correct.

15. Past messages remain confidential against future compromise ..... O Forward secrecy O Backward secrecy

16. Public key signatures yield this, assuming compromise is detected ... O Forward secrecy O Backward secrecy

17. Key revocation contributes toward achieving this ..... O Forward secrecy O Backward secrecy

18. Achieved with symmetric key evolution K → H(K) → H(H(K))..... O Forward secrecy O Backward secrecy

Protection of data while computing
Mark which method of protecting data in use applies to each statement. Exactly one answer is correct.

19. Parties have asymmetric tasks, i.e., they run different algorithms ..... O Garbled circuits O Secret sharing

20. Requires oblivious transfer to transmit information about the inputs ..... O Garbled circuits O Secret sharing

21. Protects data without using "traditional" cryptography like encryption ... O Garbled circuits O Secret sharing

Cryptography vs cryptanalysis
Mark which branch of cryptology pertains to each statement. Exactly one answer is correct.

22. Most constructions follow a divide-and-conquer approach ..... O Cryptography O Cryptanalysis

23. This is the more defense-minded branch ..... O Cryptography O Cryptanalysis

24. Two sub-branches: physics of an implementation & math of an algorithm .... O Cryptography O Cryptanalysis

25. A difference propagation table shows an S-box's vulnerability to this ..... O Cryptography O Cryptanalysis

Multiple choice questions (20 questions worth 1.5 points each, 30 points total)

For each question below, fill in the bubble(s) to the ***left*** of your desired answer(s). In this section, questions may have 0, 1, or multiple correct answers. You should treat each □ box as an independent true/false question.

Authenticated encryption modes
Mark whether each statement below applies GCM or SIV mode. Both answers may be correct.

26. Confidentiality can be achieved using counter mode ..... □ GCM □ SIV

27. An "online" mode of operation, i.e., it only requires 1 pass through the private message P ..... □ GCM □ SIV

28. Good for key wrapping, i.e., protecting the confidentiality of one key with another key ..... □ GCM □ SIV

29. Uses a custom MAC that has been built in hardware as an Intel x86 CPU instruction ..... □ GCM □ SIV

Name _____ BU ID # _____

Side channel attacks
Mark which types of side channel attacks satisfy each statement. Multiple answers may be correct.

30. A template attack exploits this side channel ..... ☐ Power ☐ (Cache) timing ☐ Padding oracle

31. A prime+probe attack exploits this side channel ..... ☐ Power ☐ (Cache) timing ☐ Padding oracle

32. Can observe this side channel remotely over a network ..... ☐ Power ☐ (Cache) timing ☐ Padding oracle

33. Code that passes test vectors may still be vulnerable to this .... ☐ Power ☐ (Cache) timing ☐ Padding oracle

34. Removing error messages from code will fix this ..... ☐ Power ☐ (Cache) timing ☐ Padding oracle

35. Attack requires Mallory to make ciphertext, not just know it ... ☐ Power ☐ (Cache) timing ☐ Padding oracle

NIST-standardized hash functions
Mark whether each statement below applies to SHA-1, SHA-2, or SHA-3. Multiple answers may be correct.

36. Accepts arbitrary-length inputs ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

37. Follows a Merkle-Damgard design ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

38. Requires a fixed-length permutation as a building block ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

39. Believed to satisfy IND$-CPA ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

40. Hash(key || message) suffices as a MAC, without the need for HMAC ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

41. Believed to be collision resistant up to the birthday bound ..... ☐ SHA-1 ☐ SHA-2 ☐ SHA-3

Hashing passwords
Mark whether each statement applies to PBDKF2, SRP, or SHA-2 with a long salt. Multiple answers may be correct.

42. Vulnerable to an offline dictionary attack ..... ☐ PBKDF2 ☐ SRP ☐ Salted SHA-2

43. Work done to dictionary attack Alice is easily reusable to attack Bob too .. ☐ PBKDF2 ☐ SRP ☐ Salted SHA-2

44. Server can safely verify password without seeing it ..... ☐ PBKDF2 ☐ SRP ☐ Salted SHA-2

45. Can be tuned to be arbitrarily slow ..... ☐ PBKDF2 ☐ SRP ☐ Salted SHA-2

Free answer questions (15 questions worth 3 points each, 45 points total)

The remaining 4 pages of this exam contain long answer questions. For each question, please explain the stated security definitions, cryptographic constructions, or attacks. It is expected that each answer should require a few sentences to address adequately, and perhaps a diagram or pseudocode as well.

If you need additional space, 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 # _____

Key agreement and ratcheting

46. Using symmetric crypto, Encrypt-then-MAC yields authenticated encryption. In this question, explain why we shouldn't use symmetric encryption with public key signatures instead. Concretely, if Alice protects a private message *P* to Bob by sending him $\text{PublicSign}_A(\text{SymEnc}_{AB}(P))$, where the signature uses Alice's private key and the symmetric encryption uses a shared key K_{AB}, show how Mallory can learn the shared encryption key K_{AB}.

47. Say Alice and Bob chat on Signal, with all communication in the Alice → Bob direction with initial chain key *K*. If Bob already received Alice's 1st and 3rd messages, then what crypto keys does Bob still have on his phone?

48. Describe Signal's public ratchet. (You do not have to explain how it connects to the symmetric ratchet.)

49. Describe the notion of *partial deniability* that Signal provides. Also, explain how Signal can achieve deniability even though it uses public key signatures (which are non-repudiable) in the public ratchet.

Name _____ BU ID # _____

Authenticated Encryption

50. List the 3 algorithms that any authenticated encryption with associated data (AEAD) scheme must provide. For each algorithm, state what it requires as input and what it provides as output (e.g., a ciphertext, a nonce, etc).

51. Define indistinguishability from random under a chosen ciphertext attack (IND$-CCA). Show the powers we give to Mallory and the task that she cannot accomplish anyway. Also, explain how it differs from IND$-CPA.

52. One advantage that SIV mode provides over GCM is *misuse resistance*. Define this property, and explain why GCM doesn't achieve it.

Side channels & other attacks

53. Suppose that Alice's password verification check runs the code on the right. It stores the real password in the clear and performs a character-by-character string comparison on any password guess. Write pseudocode showing how Mallory can find Alice's `real_pwd` by submitting password guesses and using a side channel attack.

```
// stored global const real_pwd

def password_check(pwd_attempt):
  return real_pwd == pwd_attempt
```

Name _____ BU ID # _____

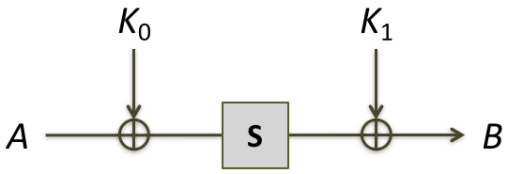
54. Consider the S-box shown on the right. It maps 3-bit inputs to 3-bit outputs. Complete the $\Delta x = 1$ row of the difference propagation table for S that is given below. Additionally, given the partial table that is shown here, state the maximum difference propagation for S. (Remember that 'difference' means xor.)

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

Output difference Δy

Input diff Δx	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0							
2	0	0	4	0	0	0	0	4
⋮				⋮				

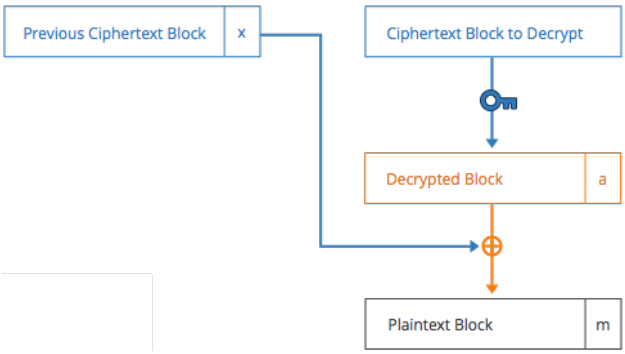
55. Consider the cipher TEST shown on the right, where all wires are 3 bits long and the S-box is the same as the one in the previous question. Suppose Mallory runs TEST on input $A = 6$ and receives output $B = 7$. Via a cache timing attack, Mallory also learns that the S-box table lookup occurred at value $x = 2$. Find the keys.



56. Consider the cipher N-TEST that contains N rounds of TEST: that is, it alternates between $N+1$ invocations of $\oplus$ and N calls to the S-box. Mallory possesses a large number of power traces on known inputs. Suppose that an implementation of the S-box has a peculiar property: it consumes substantially less power when its input is 0 than on the other 7 inputs. Describe how she can use this feature to find all $N+1$ blocks of the key.

Name _____ BU ID # _____

57. Suppose Mallory intercepts a 2-block ciphertext (shown in blue in the figure) that was produced properly via CBC mode encryption with PKCS #7 padding. Mallory observes that if she changes the final byte of the first block from *x* to *c*, then the altered ciphertext does not give a padding error. Based on this info, compute the final byte of plaintext *m* as a function of *x* and *c*.



58. Explain the difference between a rainbow table and a regular hash table when conducting a dictionary attack. Also, explain how the use of a long, randomly chosen salt will render a rainbow table useless.

Other topics

59. Alice and Bob want to know the difference between their hourly salaries. Using additive secret sharing, they send shares of their salaries to two different servers. Server 1 receives a share of 18 from Bob and 14 from Alice, and server 2 receives a share of 22 from Bob and 17 from Alice. All arithmetic is performed mod 100. Show how the servers can calculate Bob's salary minus Alice's salary, without learning either person's salary.

60. List 3 sources of entropy that computers harvest as sources for random number generation.

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.