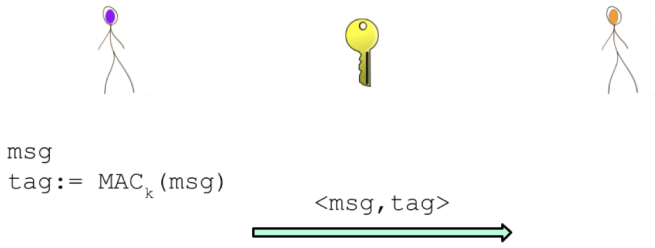
COMP435 Written Assignment 3 Name: _____

Question 1: MACs Purple sends Orange a message msg using a keyed hash message authenti- cation code (MAC_k). The MAC_k is defined as $MAC_k(msg) = h(k|msg|k)$, where h is a cryptographically secure hash function and "|" denotes concatenation. In other words, the MAC is computed by first concatenating the secret key, the message, and the key again, and then the resulting string is hashed using h. Purple computes the $tag = MAC_k(msg)$ and sends (msg, tag) to Orange.



For each of the following decide whether the statement is true or false and briefly (one sentence) explain your reasoning.

1.1. The protocol would work just as well if Purple sent only the tag without the message (True/-False and Why)

1.2. Upon receiving the communication, Orange will compute the inverse of the hash function to recover the message (True/False and Why)

1.3. Orange and Purple must both already know the key k (True/False and Why)

1.4. Upon receiving the communication, Orange will compute the hash function of msg and compare the computed value to the received tag (True/False and Why)

Question 2: Hash Functions Let h be a publicly known, cryptographically secure, collision resistant hash function that takes in messages of arbitrary length and produces a fixed-length hash value.

2.1. Given a message m, a computationally bound attacker would not be able to find a second message $m' \neq m$ such that $h(m) = h(m')$. (True/False)

2.2. There exist two messages $m' \neq m$ for which $h(m) = h(m')$. (True/False)

2.3. Since h is collision resistant, it must also be second pre-image resistant. (True/False)

Question 3: Diffie-Hellman Key Exchange Alice and Bob are using the Diffie-Hellman Key Agreement protocol to establish a shared secret key. They publicly agree on a shared prime p and primitive root for p, g. Alice privately chooses a such that a $<$ p and Bob privately chooses b such that b $<$ p. They then use these values to complete the protocol.

3.1. tWhat messages do Alice and Bob exchange next to complete the protocol? Be precise in your answer.

3.2. By the end of the protocol, does Bob know the value `a`? Briefly (one sentence) explain your answer.

Question 4: More Diffie-Hellman Alice and Bob are still working on setting up their secret key. They choose public parameters p = 19 and g = 2. Alice chooses secret a = 5. Bob chooses secret b = 9. Find A, B, and the shared secret key K. Show your work. Hint: It might be helpful to make yourself a little table of powers of 3 mod 17 to keep your math manageable!

4.1. A

4.2. B

4.3. K

Question 5: Race Conditions Consider the following attempted solution to the TOCTOU race condition we saw in lectures 11 and 12. The idea is that now each ATM does `get_bal()` and locally decides "sufficient funds?" and then later sends the result of `adjust_bal(-100)` back to the bank. Is there something wrong with this approach? If so, explain what the problem is and make a suggestion for how to fix it.