Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Score: \_\_\_\_ / 30

CPSC 42500 Homework 6: MACs, the Secure Channel

1. (2 points) The purpose of authentication protocols is to make \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ detectable. *(One word in each blank)*
2. (5 points) Use the internet to answer the following questions about the **SHA-2** family of hash functions.
3. What are the digest sizes supported by SHA-2 algorithms?
4. How many bits of collision resistance does SHA-384 provide?
5. How many rounds is the compression function for SHA-512?
6. (2 pts) What is the basic difference between SHA-224 and SHA-512/224?

1. (3 points) Using HMAC, even if an adversary can find a collision in the underlying hash function, why does this not necessarily mean that they can forge a message?

1. (4 points) You find out that your University is using an authenticated messaging system that is vulnerable to a length extension attack, because it uses an iterative hash function with the insecure MAC construction *t* = *h*(*K* || *m*). By eavesdropping on the network you intercept the following message *m* from your professor to the administration: “Set final course grade to A for J. Smith,” along with its tag *t*.

Give an example of a believable message that you could forge and send using a length-extension attack, and describe how the attack would work. Specify how you would use the hash function and what pieces of data you would send.

1. (2 points) A small company has 10 employees who all want to send authenticated messages to each other. It’s not enough to know that a message came from one of the 10 employees; it must be verifiable that a message is from one specific employee.

To solve this problem using MACs, how many different secret keys would be needed in total? Explain your answer. You only need to consider one-to-one messages; don’t worry about messages sent to an entire group.
2. (3 pts) In our definition of a secure channel, what are the two things that an eavesdropper is “allowed” to learn? Why do we allow the eavesdropper to learn them?

1. (4 pts) You are placing an order with an online retailer. To complete a purchase, your web browser sends a single encrypted, authenticated message to the web site, consisting *only* of the following information: a) your credit card information, b) the item number and quantity being ordered.
2. Say an adversary is sitting between you and the retailer, with the ability to intercept traffic and send messages. Describe an attack the adversary could carry out to “max out” your credit card. What type of attack is this?
3. What could the retailer do to prevent this attack, simply by changing what data is sent in the single encrypted, authenticated message?

1. (3 pts) The use of session keys and message numbers both serve to prevent replay attacks. Then why do we need to use both to have a secure channel?
2. (4 pts) The following sentence describes steps that are used to generate a ciphertext *c* and authentication tag *t*.

“The message number *i* is concatenated with the message and encrypted with key K*enc* to produce the ciphertext. The key K*auth* is concatenated with *i* and the message and hashed with SHA-256 to produce the tag.”

Write the definitions of *c* and *t* as a formula, using the notation we use in class and the textbook.