Computer Security Homework 5 (Due Friday 9/18/20)

1. There is a fairly new hash function standard called SHA-3. Which of the following is true of the new SHA-3 hash function?

   (a) 5-letter strings will typically have a longer SHA-3 hash than 2-letter strings

   (b) 5-letter strings will typically have a shorter SHA-3 hash than 2-letter strings

   (c) 5-letter strings will always have the same length SHA-3 hash as 2-letter strings

2. Here is the SHA-256 hash of a 53 words of English prose that I made up off the top of my head: `4c4eb81772f2a141f2c14f75ae3fe276e1d38f22a64d0b777d7af0487d08fcee`. Which of the following is true?

   (a) A highly skilled hacker could figure out the original text in a few minutes.

   (b) A highly skilled hacker could figure out the original text in a few days.

   (c) A team of highly trained security experts with access to massive amounts of computing power could figure out the original text given a few years.

   (d) There's not much hope that anyone will figure out the original text.

3. If strings `a` and `b` are 5000 characters long and equal except in their last characters, their SHA-256 hashes will be most likely be

   (a) totally different

   (b) mostly the same, but different in the last 8 bits

   (c) mostly the same, but different in a few random bits

   (d) mostly different, but the same in the last 8 bits

4. Recall that when Alice and Bob use a MAC, a shared secret key is part of the process. The purpose of that shared key that is

   (a) to encrypt the message before hashing

   (b) to guarantee the hash can't be reversed

   (c) to guarantee the hash is sufficiently random

   (d) so Bob can also verify that the message came from Alice and not someone else

5. When exchanging data in TLS, Alice and Bob do what to detect if their encrypted messages are being altered by someone in transit?

   (a) Use MACs

   (b) Digitally sign each message

   (c) Send some honeypot data that they agreed on beforehand and see if it is altered

   (d) Exchange certificates

6. True or False.

   (a) MD5 is considered to be a good hash function for use in secure applications.

   (b) SHA-256 is considered a good hash function to use for hashing passwords

   (c) Suppose we collect every sentence ever spoken by a human in history, remove any duplicates from the list, and hash everything that's left with SHA-256. There will likely be multiple sentences in the list with the same hash.

   (d) Hashing is commonly used as an encryption/decryption method.

   (e) Hashing a password is okay, but it's better to encrypt it instead.

   (f) A CA gives their seal of approval that a public key is valid by signing it with their private key.

   (g) If an attacker figures out how to produce collisions in a hash function, they can insert malware into files such that the new file has the same hash as the original.

(h) Heinold48 is a secure 48-bit hash function. If we has 1 billion different strings with this hash function, it is likely that we will get some collisions.

7. What is the name of the attack on TLS that involves an attacker tricking the parties in the TLS handshake into using weak ciphersuites that the attacker can crack?

8. Find the SHA-256 hash of the string “secure”. Please include a screenshot showing how you did it.

9. Use your browser to view the public key value used in the certificate for `msmary.edu`. Include a screenshot.

10. Suppose Alice and Bob are exchanging encrypted data with the stream cipher we wrote in class. Its code is available with this assignment. In that program, there is some ciphertext that decrypts to a message about Alice paying $100 to Bob. Play the role of Eve the eavesdropper by changing something in the ciphertext (variable `c2`) so that the decryption changes to Alice paying less money to Bob. Give a screenshot showing what you changed and the resulting decryption.

11. (a) Included with this assignment are two copies of Shakespeare’s *The Tempest*. They are exactly the same except that I changed a single character in a single place in the second copy. Compute the SHA-256 hash of each of them. [Note that the file is encoded as UTF-8. If you use Python to open it, use `open('tempest.txt', encoding='utf-8')`.] Please include a screenshot showing how you did this.

    (b) Bonus (extra credit): Find the location of the one character I did change. [Note: You can do this part and part (a) either by programming or with the command line in your favorite OS.] Please submit whatever command or code you use for this problem along with your answer.

12. Included with this assignment is a Python file. It contains a string, as well p, q, e, and d values for RSA. Add code to the file to do parts (a) and (b).

    (a) Find the SHA-256 hash of the string (in hex).

    (b) Use the *private* key to encrypt the answer from (a) with RSA using the values given in the file. You might want to convert the answer from (a) to an integer, using the `int` function with optional argument 16.

    (c) The process you performed in parts (a) and (b) is an example of what very specific modern cryptography concept from class? [Hint: the answer is not hashing or public-key cryptography.]