Computer Security Homework 6 (Due Friday 10/2/20)

1. True or False.

   (a) SHA-256 is a good hash function for storing passwords.

   (b) Encrypting passwords instead of hashing is not a good idea because anyone with access to the decryption key will get all the passwords on the system.

   (c) NIST recommends checking new user passwords against a list of common passwords.

2. Suppose it's time to change your very secure password at a site. You decide to just add the number 2 to the end of your own password. The site rejects it, saying that the password you are trying to set is the same as your old one with a digit attached. This site

   (a) is being really vigilant and doing a great job with security

   (b) is being overly picky because your password is still secure

   (c) must not be storing your passwords the right way

3. Microsoft used to have an awful password system that would break 14-character passwords into two 7-character passwords, each hashed separately, instead of just hashing the 14-character password. Which of the following is true about the time it would take a 14-character brute-force search as opposed to two 7-character brute-force searches? Assume the passwords are all uppercase letters.

   (a) It will take twice as long.

   (b) It will take 4 times as long.

   (b) It will take $2 \cdot 7 = 14$ times as long.

   (c) It will take $26 \cdot 7 = 182$ times as long.

   (d) It will take about $26^7/2 \approx 4$ billion times as long.

4. Suppose I hacked into your website and got access to the file containing all your user's passwords. I have a list on my computer of the 1,000,000 most common passwords and their hashes, and I plan to use it to instantly crack some of the weaker passwords in your password file. However, if you followed a certain important security practice with regards to passwords, then my file won't be much help, and I'll have to resort to brute-force. What is that security practice that you hopefully followed?

5. One application of public key cryptography that we covered in class is used in the Bitcoin protocol so that we know that a transaction was really made by who it says it was made by and not fraudulently by someone else. What is the name of that piece of modern cryptography?

6. What operation is used in Bitcoin to chain together a current block of transactions to previous blocks?

7. NIST is currently recommending changes to password policies that some may find controversial. What is your opinion on the two that follow? Explain briefly. I don't want you to parrot my opinion. Give your own, please.

   (a) Sites should not require that users include numbers or special characters in their passwords.

   (b) Sites should not require users to periodically change their passwords unless there was a breach.

8. Assuming a password-cracking program can check up to 10 billion passwords a second, how long will it take to crack each of the following?

   (a) A 10-character password of random uppercase letters, lowercase letters, and digits.

   (b) A 9-character password consisting of 6 lowercase letters, followed by 2 digits, followed by one of 15 possible special symbols.

9. Either write some code or use a password-cracking tool like hashcat to find the passwords whose hashes are the following. Include whatever you use to do this problem (code, hashcat commands, etc.)

(a) `b90c19d367942389189fcef814d714f1` — This is the MD5 hash of a 5-character string of lowercase letters.

(b) `e5f2c146588dc7f921a4fdfaf6cc03bd` — This is the MD5 hash of a first name followed by a year in the not-to-distant past, followed by a special character from the number row on a keyboard. An example is `Jason1999!`. There is a file of first names included with the assignment.

10. For this problem you will be mining TylerCoin. Mining TylerCoin is similar to mining Bitcoin. In this specific example, you want to find the value of a nonce so that when the nonce concatenated with the string `"whatever"` is hashed with SHA-256, the result starts with 6 zeroes. (The hash might look like 0000003a26414cddf5088387d6cf455ba458fdac3baee759d02628bd8fb2e0f3d90, except not exactly this value.)

    Find the smallest positive integer value of the nonce that works. Your answer will be something like `whatever######`, where `######` is some number. Include any code that you use to do this problem.