Password Strength Exercise:

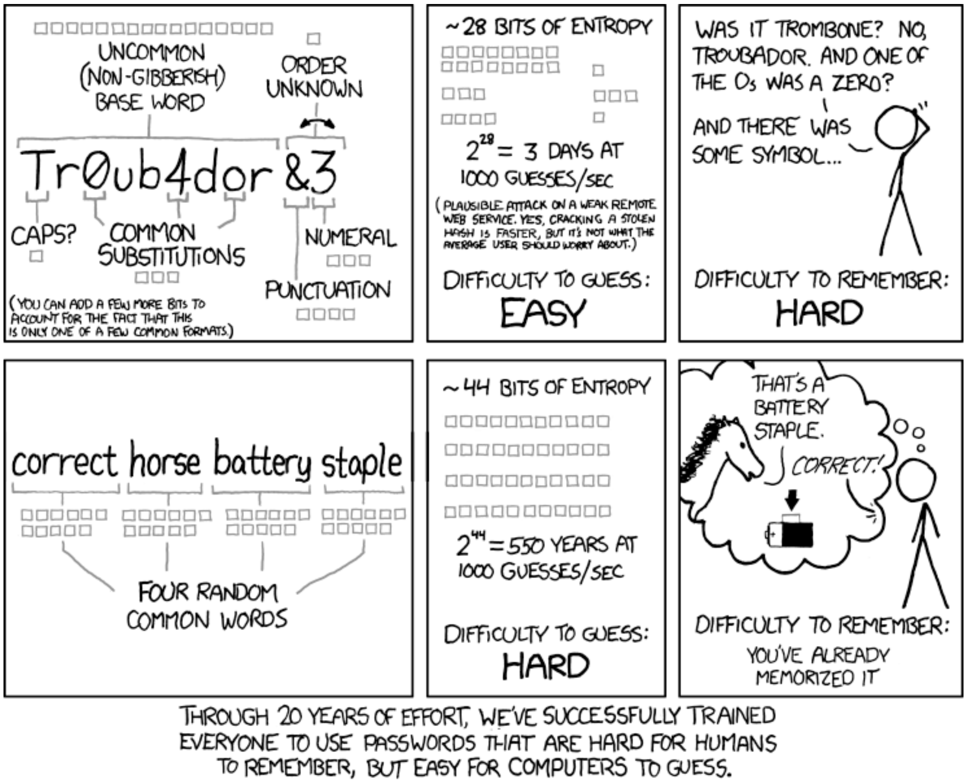
Introduction:

The objective of this assignment is to help students understand how password cracking attacks work and how you can create stronger passwords that are easier to remember but harder to guess. Password cracking attacks usually involve a computer program going through numerous possible combinations of passwords to guess the correct password. This attack is typically performed offline on leaked databases containing encrypted passwords, but it may also be performed online on website login pages.

The cracking process can be performed using either a brute-force approach, a dictionary based approach, or a combination of both. In a brute-forced approach, all possible combinations of passwords are attempted where number of possible combinations is determined by the maximum length of the password and the different types of characters used. In contrast, a dictionary based approach uses a much smaller subset of very commonly used passwords. As a result, running a brute force attack takes much longer to complete due to the insanely large number of possible combinations. In this exercise, we will learn how to strengthen our passwords against both types of cracking attacks.

Password Complexity:

Consider the comic posted by xkcd.com shown below. This comic illustrates how a strong password is not necessarily one that is difficult to remember.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

The lesson we should learn from this comic is that password complexity is not about how difficult it is to remember, but instead how difficult it is to guess by a computer program based on the amount of entropy (randomness) present in the password. In this case, a long password containing a phrase is much easier to remember but difficult to crack using a brute force attack. However, we should note that it may not be sufficiently strong against dictionary based attacks that may be specifically crafted to contain such phrases.

Creating a Strong Password:

We want to create a password that is not only difficult to brute force, but it is also difficult to guess using a dictionary, while being easy to remember and not too long. Here are some tips on creating such a password:

1. Start with a few words or a phrase that you find easy to remember. For example, think of a quote that you heard in the last TV show you watched and try to condense it into a 2-3 word long phrase.
2. Now replace some of the letters of that phrase with numbers. For example, “Alexander” can also be written as “4lexand3r”.
3. Next, try to introduce special characters. Some popular choices are “@” for “a”, “$” for “S”, and “#” for “H”.
4. Use different separator characters for the words of your phrase. For example, instead of “Destroyer of Worlds”, use something like “Destroyer_of3Worlds”.

There are many other tricks that you can apply to make a strong password. Try to use these tricks to come up with a strong password that is at most **20 characters** long, easy to remember, and that will take at least a year to crack. You may use the website Bitwarden's Password Strength Checker to test your password. Share your results with the rest of the class on this Google Spreadsheet. For obvious reasons, do not use this password on any website or computer account!