10.2 PROJECT

PASSWORDS AND SECURITY: DO HACKERS TEST ALL POSSIBILITIES?

Mark Zuckerberg, the founder and CEO of Facebook, is known to have kept "dadada" as his Twitter and Instagram passwords. Simple passwords of this type are a treat for hackers trying to gain access to an account. These passwords can be guessed in a short amount of time by what is called a dictionary attack. In this case, an intruder tests common words and their combinations until the correct password is found.

What about more secure passwords? Is it possible to simply test all possibilities for a password and gain access to someone's account? In this activity, you will estimate the time it would take to correctly guess a social media account password.

Assume that a social media platform requires your password to have exactly 8 characters selected from any of the 26 letters of the alphabet, the numbers 0 through 9, and any of the characters #, $, %, or &. In order to simplify our computations, let's assume repetitions are allowed.

1. Determine the number of distinct passwords that can be created using the requirements described above. The number is very large, so you should use a calculator or computer for your computation.

Now, let's assume that it takes 0.02 seconds to check a single possible password.

2. How many seconds would it take to check every single possible password? This approach is called a "brute force" attack.
3. How many seconds are in a year?
4. How many years would it take to check every single possible password? Round your answer to the nearest whole year.
5. Explain why it is really a worst-case scenario for the hacker for the brute force attack to take this long.
6. Do you believe hackers use the brute force attack often? Explain your reasoning.