Create a Strong Password and Evaluate its Strength

1. **Introduction:**
   Task to create a strong password, evaluate its strength, and understand password security.

2. **Password creation process:**
   I created a password that is 13 characters long, mixing uppercase letters, lowercase letters, symbols, and numbers.
   I avoided using common words or personal information".

3. **Passwords:**
   My passwords: 1. Eh$1kpsu!5TA3
   2.Ka#kp3hg%i1$A
   3.abcd1234
4. **Evaluate and Record Results:**
   1.Password: Eh$1kpsu!5TA3
   Score:100%
   Time to Crack: 422 million years
   My password is very strong because it contains 13 characters and also have lowercase, uppercase, symbols, and numbers.
   My password could not contain common password like names and common sequence.
   Improvement: NO improvement needed.

   2. Password: Ka#kp3hg%i1$A
   Score:100%
   Time to Crack: 25 million years
   My password is very strong because it contains 13 characters and also have lowercase, uppercase, symbols, and numbers.
   My password could not contain common password like names and common sequence.
   Improvement: NO improvement needed.

   3. Password: abcd1234
   Score:38%
   Time to Crack: 0 seconds
   My password is very weak because it contains 6 characters and only have and numbers.
   My password could contain common password like names and common sequence.

Improvement: Improvement needed.

Common Password Attacks

Brute Force Attack:

In a brute force attack, an attacker uses trial and error to guess a password by systematically trying every possible combination of letters, numbers, and symbols until the correct password is found.

These attacks can be performed quickly by computers and are most effective against short or simple passwords.

Automated tools are often used to accelerate the process. The fewer the characters and the less complex the password, the faster it is to crack.

Dictionary Attack:

This method leverages a precompiled list (“dictionary”) of common words, phrases, or previously leaked passwords.

Attackers systematically enter each word from the list, targeting the tendency of users to pick simple, common, or easy-to-remember passwords.

Dictionary attacks are faster than brute force attacks because they focus only on the most likely options rather than every possible combination.

How Password Complexity Affects Security

Stronger Defense: Complex passwords are much harder to guess or crack because they use a mix of uppercase, lowercase, numbers, and symbols, increasing the total number of possible combinations.

Longer Crack Times: As length and complexity increase, both brute force and dictionary attacks require exponentially more time and computing power, often making attacks impractical.

Less Predictable: Complex passwords that avoid common words, patterns, and personal information are less likely to appear in attackers' dictionaries, making dictionary attacks far less effective.

Higher Entropy: Complexity increases entropy (unpredictability), reducing the chances of successful password guessing.