Password Strength Checker

DISCRETE PROJECT

Today's Objectives

WHAT IS A PASSWORD?

A password is like a secret code that only you know. You use it to open or unlock things that are private, like your phone, Facebook account, or email. When you enter the correct password, it proves that you are the right person allowed to see that information.

IMPORTANCE OF PASSWORD STRENGTH

Enhances security by increasing the difficulty of brute-force attacks and also other types of attacks.

OUR GOAL TODAY

Using discrete mathematics principles to analyze and implement a password strength checker.

Real-World Applications and Future Considerations

- ONLINE ACCOUNT SECURITY
- BANKING AND FINANCIAL PLATFORMS
- CORPORATE AND ENTERPRISE SYSTEMS
- CYBERSECURITY TRAINING AND AWARENESS
- SECURING SOCIAL IDENTITY OF PEOPLE

Connection to Discrete mathematics

PROBABILITY

likelihood chances of guessing the password. Password with more chance of guessing have more probabilty

COMBINATIONS

Combinations are all the different ways you can choose characters for a password, no matter the order. If you have letters, numbers, and symbols, combinations show how many unique passwords you can create from them.

PERMUTATION

In a password checker, permutations are the different ways characters can be arranged. Stronger passwords have more complex combinations and less predictable patterns.

LOGICAL OPERATORS

Which can be used for measuring the strength criteria of any password.

Password Strength Criteria Using Logical Operators

AND OPERATOR (∧)

Password meets all requirements (e.g., uppercase and lowercase).

OR OPERATOR (∨)

Password has at least one requirement (e.g., either uppercase or digits).

NOT OPERATOR(!)

Exclude easy sequences (e.g., "123456").

PASSWORD IS STRONG IF: LENGTH 8 ∧ CONTAINS UPPERCASE ∧ CONTAINS LOWERCASE ∧ CONTAINS SPECIAL CHARACTER

Combinations Of Passwords

- FOR A PASSWORD OF LENGHT N
  - LOWERCASE LETTERS: $(26)^N$
  - UPPERCASE LETTERS: $(26)^N$
  - DIGITS: $(10)^N$
  - SPECIAL CHARACTERS: E.G WE ARE GETTING 10 . SO $(10)^N$

- FOR EXAMPLE : IF WE ARE MAKING A PASSWORD OF 8 CHARACTERS THE TOTAL COMBINATIONS WILL BE

$$(26+26+10+10)^8$$

TOTAL POSSIBLE PASSWORDS: 722,204,136,308,736

Probability of Guessing a Password

RANDOM GUESSING ATTACK

IF someone is guessing in the first try the probability of it will be

1/Total combinations

ENTROPY OF PASSWORD:

- Measures uncertainty:
  Entropy=log2(Total Combinations)

- A high entropy indicates a lower probability of guessing.

Complexity Analysis and Big-O Notation (worst case)

- For a password of length n, the checker runs in O(n) as it examines each character.

- Worst case: all criteria checked without meeting, still O(n).

Password Strength Checker Algorithm

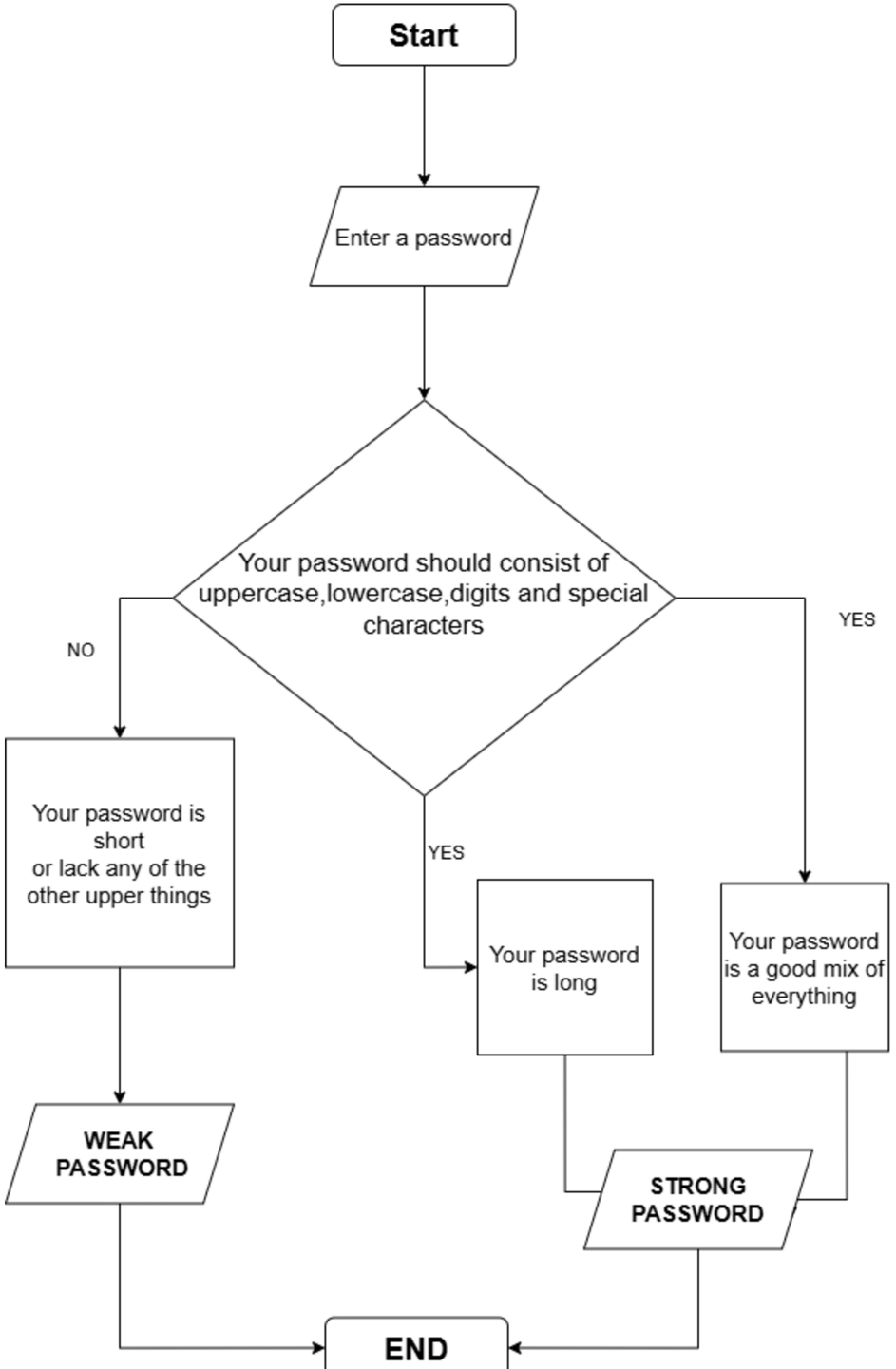
CHECK LENGTH: ENSURE PASSWORD HAS A MINIMUM LENGTH N.

UPPERCASE CHECK: X PASSWORD X UPPERCASE

LOWERCASE CHECK: Y PASSWORD Y LOWERCASE

DIGITS CHECK: Z PASSWORD Z DIGITS

LOGICAL OUTPUT: PASSWORD PASSES IF IT MEETS ALL CRITERIA, INDICATING STRONG, MEDIUM, OR WEAK STATUS.


Start
Enter a password
Your password should consist of uppercase,lowercase,digits and special characters
NO
YES
YES
Your password is short
or lack any of the other upper things
Your password is long
Your password is a good mix of everything
WEAK PASSWORD
STRONG PASSWORD
END

DEMO

USING PREVIOUS SLIDE ALGORITHM
WE DESIGNED A PASSWORD STRENGHT CHECKER AND GENERATOR

Conclusions

- Discrete mathematics provides tools for analyzing password strength.
- Password strength checking combines combinatorics, probability, and logical operations.
- Strong passwords can be systematically enforced by applying discrete mathematical principles.

Q&A

Thanks!