Lab05

Which passwords were found and how quickly?

John the Ripper quickly found Password1, qwerty123, letmein, and Summer2024. All within a few seconds, since they are common words that appear in dictionary lists.

Which strong password did the program not find? Why?

The password My$Strong&Pass2024 was not found because it is long, includes uppercase and lowercase letters, numbers, and special symbols, and does not appear in the common wordlist used by the program.

How does the security score increase as you increase the length?

Password strength increases exponentially with each additional character. A longer password dramatically raises the number of possible combinations, making brute-force or dictionary attacks much slower.

How do special characters affect the score?

Special characters add complexity and increase the number of possible combinations, which makes the password harder to guess or find in pre-built wordlists.

How is a “passphrase” scored compared to a classic password?

A passphrase is usually much longer and easier to remember, which gives it a higher security score. For example, BlueTigerEatsPizza is more secure than a short password like P@ss12! because of its length.

Which password would you recommend for everyday use and why?

I would recommend using a long passphrase (at least 12–16 characters) that combines random words, numbers, and symbols for example:

Sunny$River_Books2025

It’s both strong and memorable, offering excellent protection against brute-force and dictionary attacks.