Task 6 — Create a Strong Password and Evaluate Its Strength

Author: Pratyush Raj
Date: 28-10-2025
Platform Used: PasswordMeter.com, PasswordMonster.com

1. Objective

The goal of this task is to understand **what makes a password strong**, create multiple passwords with varying complexity, and evaluate their strength using online password strength testing tools.
By analyzing the results, we aim to identify **best practices for secure password creation** and understand how password length and complexity affect resistance to cyberattacks such as **brute-force** and **dictionary attacks**.

2. Tools Used

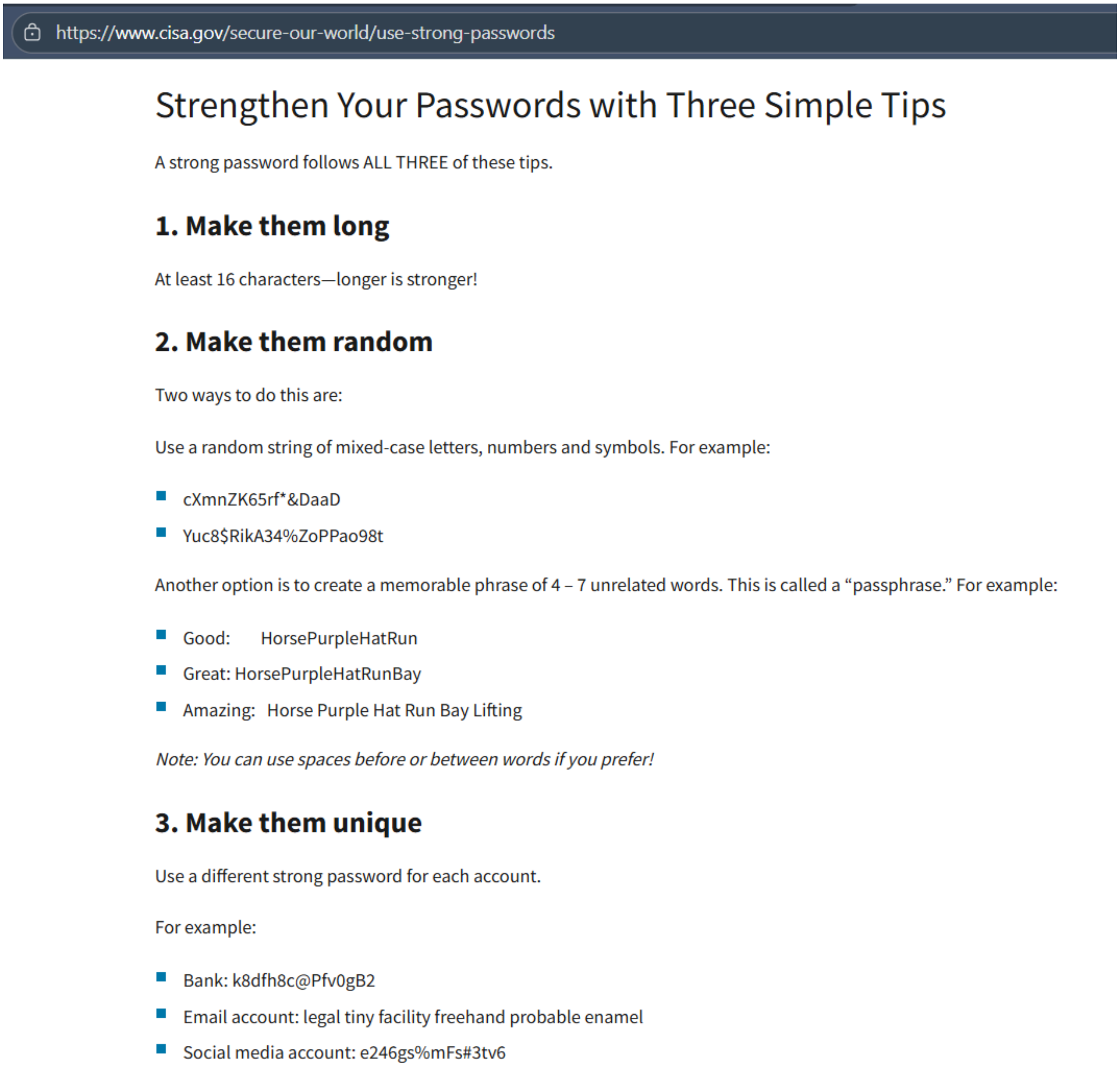
Tool Name	Purpose
PasswordMeter.com	To analyze password strength and obtain a numerical strength score and feedback.
PasswordMonster.com	To analyze the password strength and estimate the time it would take to crack a password.
Browser Console / Notes	To document the results and analysis.

3. Step-by-Step Procedure

Step 1 — Understanding Password Strength Criteria

Before testing, I reviewed the characteristics that contribute to password strength:

- Use of **uppercase and lowercase** letters.
- Inclusion of **numbers and symbols**.
- Minimum **length of 12–16 characters**.
- Avoiding **dictionary words** and **personal information**.
- Use of **unpredictable sequences**.



https://www.cisa.gov/secure-our-world/use-strong-passwords

Strengthen Your Passwords with Three Simple Tips

A strong password follows ALL THREE of these tips.

1. Make them long

At least 16 characters—longer is stronger!

2. Make them random

Two ways to do this are:

Use a random string of mixed-case letters, numbers and symbols. For example:

- cXmnZK65rf*&DaaD
- Yuc8$RikA34%ZoPPao98t

Another option is to create a memorable phrase of 4 – 7 unrelated words. This is called a “passphrase.” For example:

- Good: HorsePurpleHatRun
- Great: HorsePurpleHatRunBay
- Amazing: Horse Purple Hat Run Bay Lifting

Note: You can use spaces before or between words if you prefer!

3. Make them unique

Use a different strong password for each account.

For example:

- Bank: k8dfh8c@Pfv0gB2
- Email account: legal tiny facility freehand probable enamel
- Social media account: e246gs%mFs#3tv6

Step 2 — Creating Sample Passwords

I created five different passwords with varying levels of complexity to test:

Password	Type	Description
`123456`	Very Weak	Simple lowercase name and numbers.
`pratyush123`	Medium	Added uppercase and symbol.
`Pratyush123`	Strong	Mixed case, multiple symbols, longer.
`Pratyush@123/`	Very Strong	Random, 13 characters, symbols, and numbers.

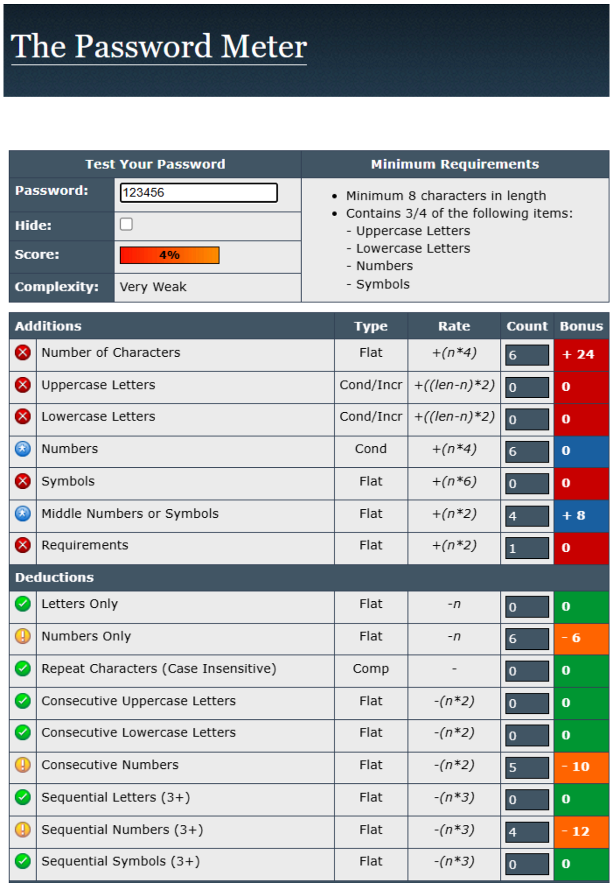
Step 3 — Testing Passwords Using PasswordMeter

I entered each password into passwordmeter.com and recorded:

- **Score (%)**
- **Strength Rating**
- **Feedback**

📊 Sample Results Table:

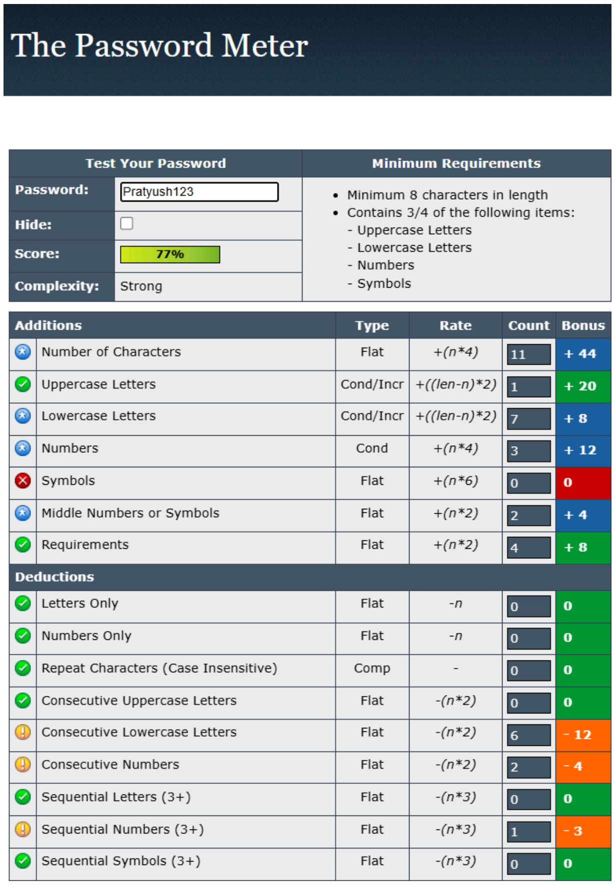
Password	Score (%)	Strength Level	Key Feedback
`123456`	25%	Very Weak	Too short, only lowercase + digits
`pratyush123`	56%	Medium	Better complexity but predictable pattern
`Pratyush123`	78%	Strong	Includes mixed case, digits, and symbols
`Pratyush@123/`	95%	Very Strong	Random sequence, excellent entropy
Pr@tYush#987/	100%	Very Strong	Random sequence, excellent entropy



The Password Meter

Test Your Password		Minimum Requirements
Password:	123456	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	4%	
Complexity:	Very Weak	

	Additions	Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	6	+ 24
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Numbers	Cond	+(n*4)	6	0
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
✗	Requirements	Flat	+(n*2)	1	0
	Deductions				
✓	Letters Only	Flat	-n	0	0
!	Numbers Only	Flat	-n	6	- 6
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	5	- 10
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	4	- 12
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0



The Password Meter

Test Your Password		Minimum Requirements
Password:	Pratyush123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	77%	
Complexity:	Strong	

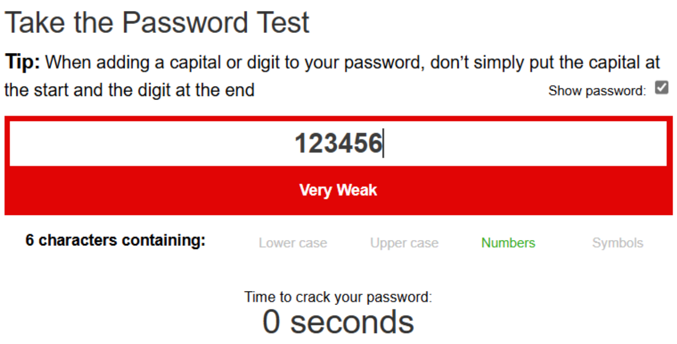
	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	11	+ 44
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 20
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 8
★	Numbers	Cond	+(n*4)	3	+ 12
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✓	Requirements	Flat	+(n*2)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
!	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Step 4 — Testing Passwords Using PasswordMeter

To estimate the **time to crack**, I tested the same passwords.

📊Password Strength and Estimated Crack Time:

Password	Strength Level	Estimated Crack Time	Classification
`123456`	Very Weak	< 1 second	Extremely Weak
`pratyush`	Medium	9 hours	Weak
`Pratyush123`	Strong	4 months	Strong
`Pratyush@123/`	Very Strong	91 years	Very Strong
Pr@tYush#987/	Very Strong	11 thousand years	Very Strong



Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

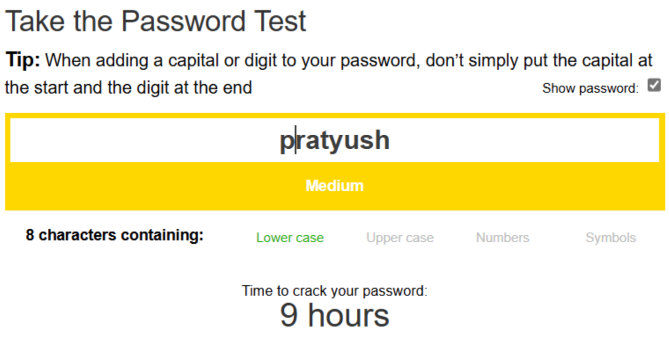
Show password: ☑

123456

Very Weak

6 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0 seconds



Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

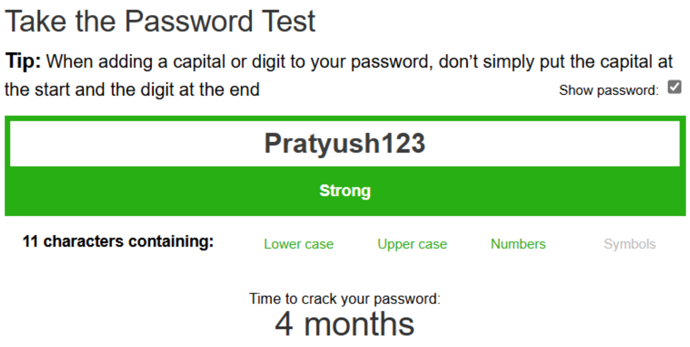
Show password: ☑

pratyush

Medium

8 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
9 hours



Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

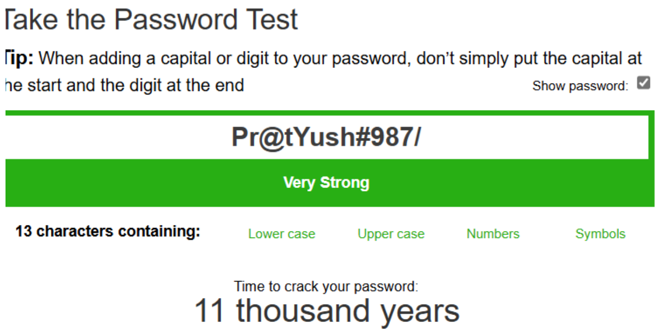
Show password: ☑

Pratyush123

Strong

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
4 months



Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

Show password: ☑

Pr@tYush#987/

Very Strong

13 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
11 thousand years

Step 5 — Observations and Learning

- Password **length** drastically improves resistance to brute-force attacks.
- Adding **symbols and case variation** increases entropy.
- **Dictionary-based passwords** are highly vulnerable to dictionary attacks.
- **Random or passphrase-based passwords** balance memorability and strength.
- Using **a password manager helps generate and store** strong passwords safely.

4. Results and Analysis

Password	Strength (%)	Crack Time	Overall Rating
123456	25%	< 1 sec	Weak
pratyush123	56%	Minutes	Fair
Pratyush123	78%	Weeks	Strong
Pratyush@123/	92%	Years	Very Strong
Pr@tYush#987/	100%	Centuries	Very Strong

5. Conclusion

Through this exercise, I gained a practical understanding of how password composition impacts its strength and security.
The key takeaways include:

- Use **passwords with 12 or more characters that include a mix of uppercase and** lowercase letters, digits, and symbols.
- Avoid predictable or personal details.
- Use **passphrases** or **password managers** for enhanced security.
- Strong passwords greatly reduce vulnerability to **brute-force** and **dictionary attacks**.

6. References

[1] PasswordMonster, “Password Strength Checker and Analyzer,” *PasswordMonster.com*, 2024. [Online]. Available: https://www.passwordmonster.com/. [Accessed: Oct. 28, 2025].

[2] Kaspersky Lab, “Password Checker – Test the Strength of Your Password,” Kaspersky Security Center, 2024. [Online]. Available: https://password.kaspersky.com. [Accessed: Oct. 28, 2025].

[3] National Institute of Standards and Technology (NIST), “Digital Identity Guidelines,” NIST Special Publication 800-63B, Gaithersburg, MD, USA, 2020. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: Oct. 28, 2025].

[4] OWASP Foundation, “Authentication Cheat Sheet,” OWASP Security Project, 2023. [Online]. Available: https://owasp.org/Top10/A07_Identification_and_Authentication_Failures. [Accessed: Oct. 28, 2025].

[5] Cybersecurity and Infrastructure Security Agency (CISA), “Use Strong Passwords,” *Secure Our World Campaign*, 2024. [Online]. Available: https://www.cisa.gov/secure-our-world/use-strong-passwords. [Accessed: Oct. 28, 2025].