Task 6: Password Strength Evaluation

Objective

To create and evaluate the strength of multiple passwords using online tools and understand how password complexity affects security.

Tools Used

• https://passwordmeter.com

Passwords Tested

Password	Score / Result	Feedback Summary
atul123	Weak (10%)	Too short, lacks symbols, common pattern
Atul@123	Medium (50%)	Has uppercase, symbol, numbers, moderate length
AtuL#983^x	Strong (90%)	Good length, uses varied character types
Monkey!Guitar@Rain9	Very Strong (100%)	Long passphrase, complex and unique

Observations & Best Practices

- Use a combination of uppercase, lowercase, numbers, and special characters.

- Longer passwords are generally more secure.

- Avoid using dictionary words, personal information, or common patterns.

- Passphrases provide both strength and memorability.

Common Password Attacks

• Brute Force Attack – Tries every possible combination until the correct one is found. Stronger passwords take longer to crack.

• Dictionary Attack – Attempts passwords using a precompiled list of common words or previously leaked credentials.

Conclusion

This evaluation shows how password strength can be significantly improved with simple techniques like adding symbols, using passphrases, and increasing length. Strong, unique passwords play a vital role in defending against common attack methods.