# Password Strength Evaluation Report

## Objective

The objective of this task is to understand how password complexity affects strength, recognize common weaknesses, and learn best practices for securing passwords by evaluating them with online password checkers.

## Passwords Tested and Results

The following passwords were tested using an advanced password strength tool with detailed stats from screenshots:

| **Password** | **Length** | **Entropy** | **Strength** | **Brute Force Crack Time (GPU Farm)** | **Screenshot** |
| --- | --- | --- | --- | --- | --- |
| password123 | 11 | 57 bits | Moderate | 4 minutes | Screenshot1.png |
| India@2025 | 10 | 66 bits | Moderate | 9 days | screenshot2.png |
| Mai!nG01 | 8 | 53 bits | Moderate | 1 minute | Screenshot3.png |
| fK!@12uLM | 9 | 59 bits | Moderate | 3 days | Screenshot4.png |
| Ru$h!4P@ssW0rd | 14 | 92 bits | Strong | 3 million years | screenshot5.png |
| X3!m#v9L\*2wR | 12 | 79 bits | Moderate | 321 years | Screenshot6.png |
| KswjS1MX17a0-DxktdS | 65 | 427 bits | Very Strong | Trillions of years | screenshot7.png |

## Detailed Feedback & Analysis

* **Moderate Strength Passwords** (e.g., "password123", "India@2025"):
  + Typically short to medium length with some character variety.
  + Vulnerable to brute force and optimized attacks within minutes to days.
  + Common patterns and missing character types lower strength.
* **Strong Passwords** (e.g., "Ru$h!4P@ssW0rd"):
  + Longer with a good mix of symbols, numbers, uppercase, and lowercase letters.
  + Resilient to attacks for millions of years on modern hardware.
* **Very Strong Passwords** (e.g., "KswjS1MX17a0-DxktdS"):
  + Very long (65 characters) and highly complex.
  + Entropy level at 427 bits.
  + Unbreakable within any feasible time frame by brute force or optimized attacks.

## Insights

* Password length and complexity have an exponential effect on strength and crack times.
* Entropy is the best single metric; higher entropy means exponentially better security.
* Adding symbols, upper and lowercase letters, and digits improves entropy and strength.
* Avoid simple patterns, repeated sequences, or predictable endings.
* Passwords under 10 characters—even with complexity—can still be brute forced in days or less.
* Passwords over 14 characters with high variety become practically unbreakable by standard attacks.

## Best Practices for Secure Passwords

* **Use at least 12-16 characters.** Longer is vastly stronger, as seen in the 65-character password.
* **Include a mix of character types:** uppercase, lowercase, digits, and symbols.
* **Avoid common words or obvious patterns.**
* Use unique passwords for each service and consider a password manager for generating and storing complex passwords.
* Regularly update passwords and check them against breach databases to avoid reused or leaked passwords.

## Conclusion

The password strength evaluation clearly shows that longer and more complex passwords exponentially improve security against brute force and optimized attacks. Short or common passwords remain highly vulnerable despite adding symbols or numbers.

These tool-based measures and attack time estimates help users create more secure passwords by understanding the practical impact of their choices.