**🧾 Task-6 Password Strength Evaluation Report**

**🔍 Password Summary**

* **Score**: **77%**
* **Complexity**: **Strong**
* **Length**: 13 characters

**✅ Additions (Positive Factors)**

| **Metric** | **Count** | **Bonus Points** | **Notes** |
| --- | --- | --- | --- |
| Number of Characters | 13 | +52 | Longer passwords add significant strength |
| Lowercase Letters | 8 | +10 | Sufficient usage of lowercase |
| Numbers | 4 | +16 | Enhances complexity |
| Symbols | 1 | +6 | Adds uniqueness |
| Middle Numbers/Symbols | 4 | +8 | Placement in the middle boosts security |
| Requirements Met (4 of 5) | 4 | +8 | Satisfied minimum character type and length criteria |

**❌ Deductions (Weaknesses)**

| **Issue** | **Count** | **Penalty** | **Notes** |
| --- | --- | --- | --- |
| Repeat Characters | 7 | -3 | Repeated characters reduce unpredictability |
| Consecutive Lowercase | 7 | -14 | Long sequences of lowercase letters are predictable |
| Consecutive Numbers | 3 | -6 | May indicate a pattern or guessable sequence |

**📈 Analysis Summary**

* The password is well-structured with a **strong length** and diverse character types (lowercase, numbers, symbol).
* It avoids common pitfalls like using only letters or only numbers.
* However, **too many consecutive lowercase letters** and **some repetition** slightly weakened the score.
* A single **uppercase letter** could further improve balance and increase the score.

**💡 Recommendations for Improvement**

* Break up **consecutive lowercase characters** (e.g., abcdefg → Ab#cDef1g).
* Add at least **1 uppercase letter**.
* Introduce **another symbol**, especially in the middle, to increase entropy.
* Minimize character repetition if possible.

**🏁 Conclusion**

* Your password is classified as **strong** and meets most security best practices.
* With **minor improvements**, you could push it toward an **exceptional** rating (85–100%).