Task 4: Password Security & Analysis Report

Name: Mohammed Fadil PK **Date:** January 20, 2026

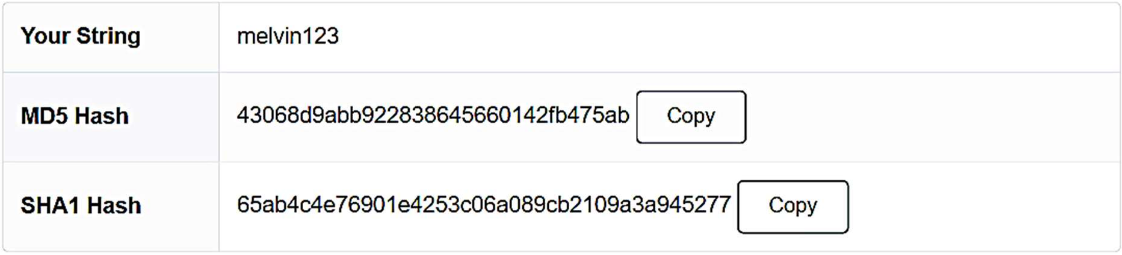
1. Introduction

Password security relies on **Hashing**. Unlike encryption, hashing is a one-way process used to securely store passwords. For this task, I generated MD5 hashes and demonstrated how weak passwords can be easily "cracked" using dictionary attacks.

2. Practical Demonstration

A. Generating a Hash (MD5)

- **Concept:** When a user creates a password, the system converts it into a "Hash" (a fixed-length string of characters).
- **Action:** I took the weak password melvin123 and converted it into an MD5 hash.
- **Hash Result:** 43068d9abb922838645660142fb475ab

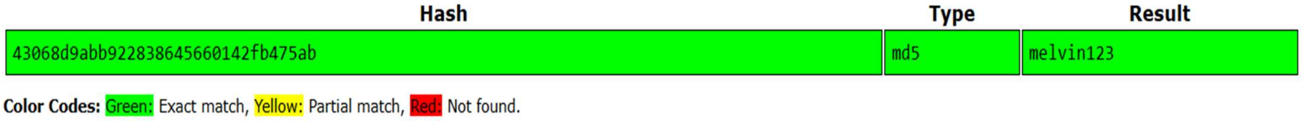


Your String	melvin123
MD5 Hash	43068d9abb922838645660142fb475ab
SHA1 Hash	65ab4c4e76901e4253c06a089cb2109a3a945277

Fig 1: Generating an MD5 hash for the weak password "melvin123"

B. Cracking the Hash (Dictionary Attack)

- **Concept:** Attackers use "Rainbow Tables" (huge lists of pre-calculated hashes) to find matches.
- **Action:** I used an online cracking tool (CrackStation) to look up the hash. Since melvin123 is a common password, the tool found it instantly.
- **Lesson:** Complex passwords (with symbols/numbers) are harder to find in these lists.



Hash	Type	Result
43068d9abb922838645660142fb475ab	md5	melvin123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Fig 2: Successfully cracking the MD5 hash using a dictionary attack on CrackStation

3. Security Analysis (Best Practices)

- **Weakness of MD5:** MD5 is an old hashing algorithm that is considered "broken" because it is too fast/easy to crack. Modern systems should use **bcrypt** or **Argon2**.
- **MFA (Multi-Factor Authentication):** Even if a hacker cracks a password, MFA stops them by asking for a second code (OTP). This is the single most important defence against password attacks.

4. Interview Questions

1. **What is the difference between Hashing and Encryption?**
    - **Encryption:** Two-way. Data is scrambled but can be unscrambled with a key.
    - **Hashing:** One-way. Data is scrambled and *cannot* be reversed.
2. **What is a Brute Force Attack?** Trying every possible combination of characters (aaaa, aaab...) until the correct password is found.
3. **Why is MFA important?** It adds a second layer of defence. If a password is stolen (something you know), the attacker still needs the phone/OTP (something you have) to log in.