Introduction

In this class activity, we explored the process of generating hash values for both weak and strong passwords using various hashing algorithms. We used the online tool to generate hash values and then attempted to crack these hashes using online crackers like, Crack Station.

Steps Performed

1. **Generating Hash Values:**

   Used the password 1234# (weak password) and generated hash values using the following algorithms along with the hash values they generated:

   - MD5: F97223DDDF692DFD903332BBEC69D407
   - SHA1: 4A413D247AB68EF153B2EE18855F82D38EDD57C0
   - SHA256: 9634B18AF2C07DBEEA71ABF88E654381B59685A5626695DA53C577C3F74B82A8
   - SHA512: CAF79E4C6F460A99D443F5986E8F2D42EE9459CEB39120EE1BD9F10A38F2492B5FFE6A3AFDF823709B7ADCB82A4C05AB77C28BD45DAFC764CBE38E22E6F10B20

2. **Observations on Hash Sizes:**

   MD5: Produces a 32-character hash.

   SHA1: Produces a 40-character hash.

   SHA256: Produces a 64-character hash.

   SHA512: Produces a 128-character hash.

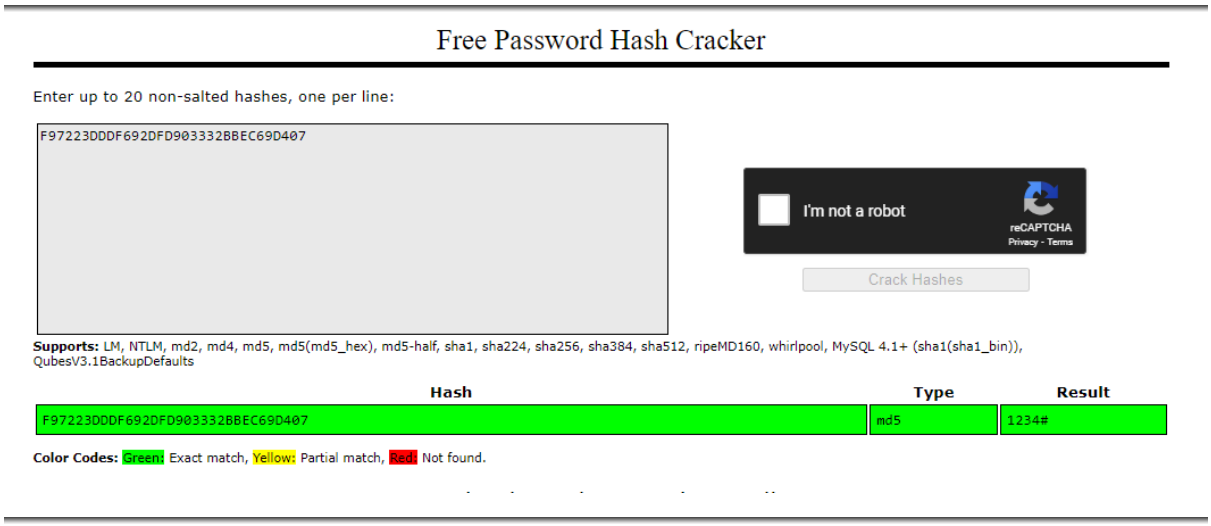
The size of the hash value increases with the complexity of the hashing algorithm.

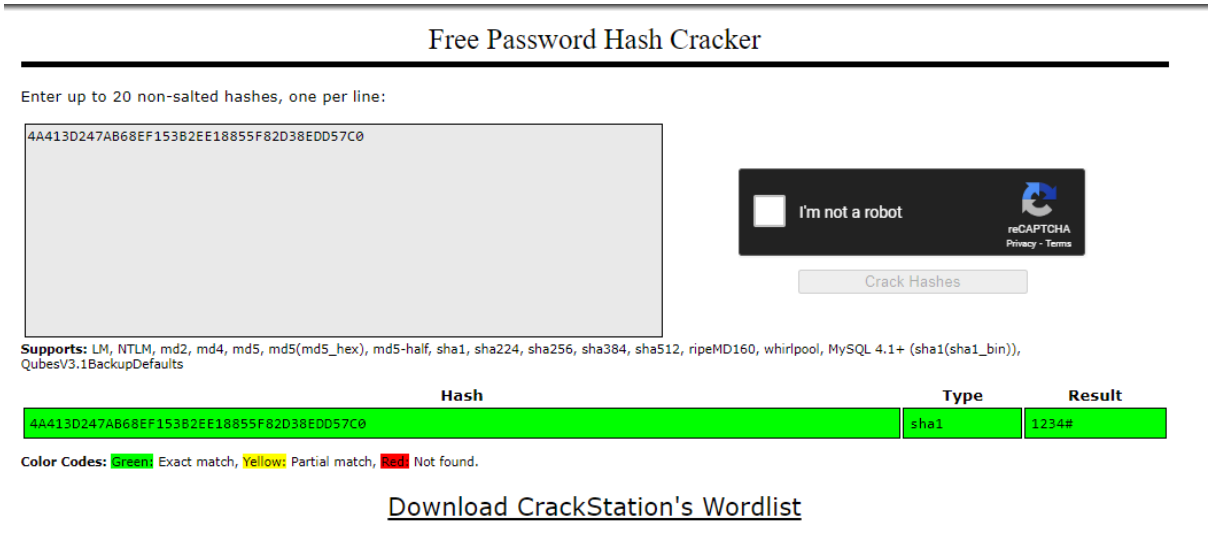
3. **Cracking the Hashes:**

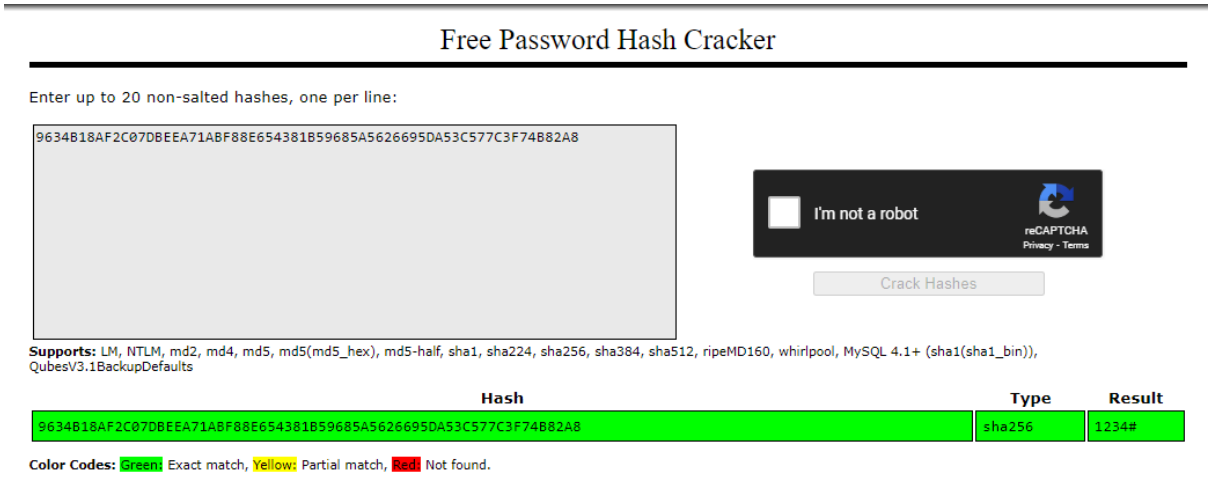
Attempted to crack the hash values using online crackers.

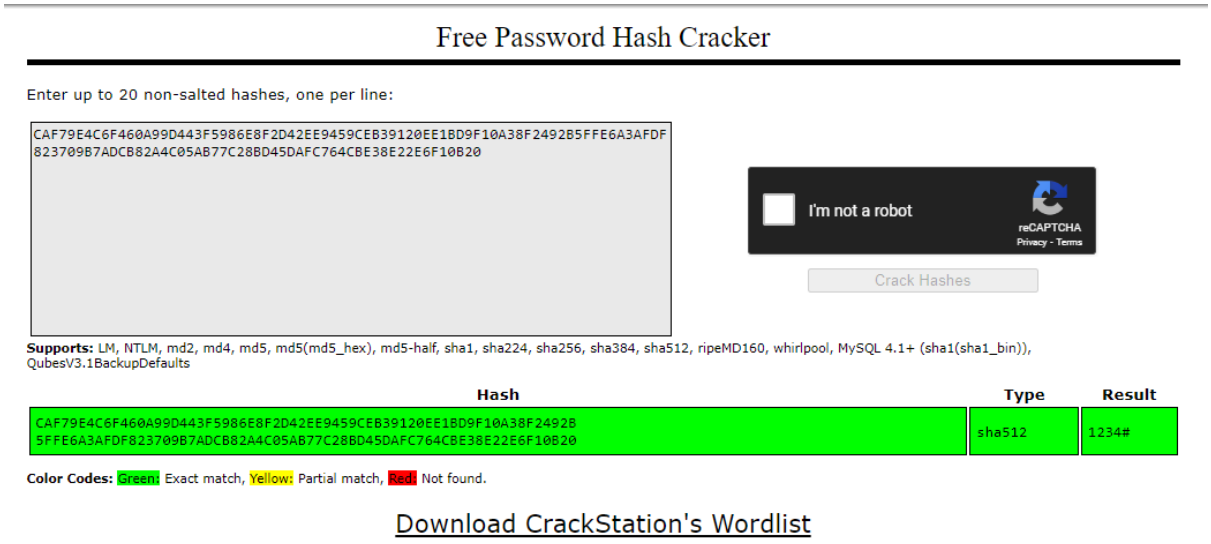
Simple Password (`1234#`):

- Successfully cracked the hashes generated by MD5, SHA1, SHA256, and SHA512 as shown in the screenshots below.









Complex Passwords (e.g., #a1b2C3D4):

When the password started with a letter or special symbol, none of the hash values for MD5, SHA1, SHA256, and SHA512 were successfully cracked.

Increasing the length of the password also resulted in the hashes remaining uncracked.

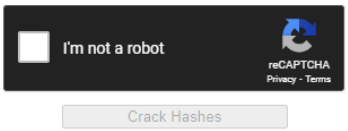
See the screenshot below

MD5

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
C5E55D82F2E1694ADBD39648F2A46D94
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
C5E55D82F2E1694ADBD39648F2A46D94	Unknown	Not found.

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

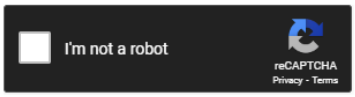
Download CrackStation's Wordlist

SHA1

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
C55680DE829B80A49D7BA68015F836E28A7A9CDB
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
C55680DE829B80A49D7BA68015F836E28A7A9CDB	Unknown	Not found.

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

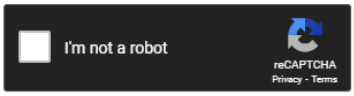
Download CrackStation's Wordlist

SHA256

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
925C8585F1033CD2DA3AC811981102AE48E2E927BE7C7B91A773A4304AA01D8D68CFB2D0D89
2898CD09A6776C86357B11C8C5CC8C134AD6FE865AE4D1937AA25
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
925C8585F1033CD2DA3AC811981102AE48E2E927BE7C7B91A773A4304AA01D8D 68CFB2D0D892898CD09A6776C86357B11C8C5CC8C134AD6FE865AE4D1937AA25	Unknown	Not found.

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

SHA512

Conclusion

The activity demonstrated the following key points:

1. **Hash Value Sizes:** The size of hash values increases with the complexity of the hashing algorithm. MD5 generates the smallest hash, while SHA512 generates the largest.
2. **Crackability of Weak Passwords:** Weak passwords (e.g., 1234#) are easily cracked regardless of the hashing algorithm used. This indicates that weak passwords do not provide sufficient security even when hashed.
3. **Effectiveness of Strong Passwords:** Stronger passwords that start with letters or special symbols, or are of increased length, significantly reduce the likelihood of successful hash cracking. None of the hashes for complex passwords were cracked in this activity, highlighting the importance of using strong, complex passwords for security.

This activity underscores the importance of selecting strong passwords and using robust hashing algorithms to ensure data security.