How passwords are stored (hashing vs encryption)

Encryption (NOT ideal for passwords)

- Can be decrypted back
- If key leaks → passwords exposed

Hashing (best)

- Password → hash (one-way)

Hash Type	Length	Security
MD5	32 chars	Weak
SHA-1	40 chars	Weak
SHA-256	64 chars	Better
bcrypt	Variable	Strong

MD5 and SHA-1 are weak and fast to crack.

- Generate password hashes.

Use **online hash generator**

1. Go to any **Online Hash Generator**
2. Enter a test password like:

```
hello123
```

3. Generate:

- MD5
- SHA-1
- SHA-256

Save the hashes in a text file.

Identify hash type

Use:

- Online Hash Identifier
  OR
- Length + format

Example:

`5f4dcc3b5aa765d61d8327deb882cf99 → MD5`

“Hash was identified as MD5 based on length and structure.”

Dictionary Attack

- Uses common passwords
- Example list:

```
password
123456
admin
hello123
```

✔ Fast
❌ Fails on strong passwords

Brute Force Attack

- Tries all combinations
- Example:

`aaa → aab → aac ...`

✔ Guaranteed eventually
❌ Very slow

- Why weak passwords fail

Weak passwords:

- Short length
- Common words

- No symbols
- Predictable patterns

Example:

password123 → `cracked easily`

Strong passwords:

`P@ssW0rd!9X#` → `very hard`

MFA (Multi-Factor Authentication)

What is MFA?

Using **more than one verification method**:

1. Password (something you know)
2. OTP / Authenticator app (something you have)
3. Fingerprint / Face (something you are)

✔ Even if password is stolen, account stays safe.

- **Strong Authentication Recommendations**

1. Use long passwords (12–16 characters)
2. Avoid common words
3. Use symbols, numbers, uppercase
4. Never reuse passwords
5. Enable MFA
6. Use password managers
7. Avoid storing passwords in plain text
8. Use bcrypt or Argon2 for hashing

Password Security Analysis Report

Title: Password Security & Authentication Analysis.

Objective:
To understand password storage, common attacks, and security defenses.

Tools Used:
Online Hash Generators, Hash Identifiers
(Conceptual study of Hashcat & John the Ripper)

Password Storage Analysis:
Passwords are stored using hashing techniques to prevent recovery of original passwords.

Hash Types Studied:
MD5, SHA-1, SHA-256, bcrypt

Attack Techniques Studied:

- Dictionary Attack
- Brute Force Attack

Observations:

- Weak passwords are easily guessed
- MD5 and SHA-1 hashes are insecure
- Longer passwords increase cracking difficulty

Multi-Factor Authentication:
MFA adds an extra security layer and prevents unauthorized access even if passwords are compromised.

Conclusion:
Strong passwords and MFA are essential for protecting user accounts from attacks.