1. How passwords are stored (Hashing vs Encryption)

Websites **do not store passwords in plain text**.
Instead, they convert the password into another form.

- **Hashing** ○ One-way process
  - Once hashed, you **cannot get the original password back**
    - This is the correct and safe method
  - Example: `password123 → 482c811da5d5b4bc6d497ffa98491e38`
- **Encryption** ○ Two-way process
  - Password can be decrypted using a key ○ If the key is stolen, all passwords are exposed ○ Less safe than hashing for passwords

Conclusion: Passwords should always be **hashed, not encrypted**.

---

2. Different hash types (MD5, SHA-1, bcrypt)

- **MD5**
  - Very fast ○ Easy to crack ○ Not secure today
- **SHA-1**
  - Slightly better than MD5 ○ Still broken and unsafe
- **bcrypt** ○ Slow on purpose ○ Uses salt (extra random data) ○ Very hard to crack ○ Used by modern secure systems

Best choice: bcrypt (or similar like Argon2).

---

3. Generating password hashes

When a user creates a password:

1. The password is sent to the server
2. It is converted into a hash
3. Only the hash is saved in the database

Example:

- Password: `Admin@123`
- bcrypt hash: `$2b$10$K9g...`

Even if two users use the same password, **their hashes will be different** due to salting.

---

4. Cracking weak hashes using wordlists

- A **wordlist** is a file with common passwords
  Example: `123456`, `password`, `admin` •
  The attacker:
  1. Takes each word from the list
  2. Hashes it
  3. Compares it with the stolen hash

If it matches → password is cracked

Weak passwords are cracked in seconds.

---

5. Brute force vs Dictionary attacks

- **Brute force attack** ○ Tries every possible combination
  - Very slow
  - Example: aaaa → aaab → aaac
- **Dictionary attack** ○ Uses common passwords ○ Much faster ○ Very effective on weak passwords

Most real attacks use **dictionary attacks first**.

---

6. Why weak passwords fail

Weak passwords:

- Are short
- Use common words
- No special characters • Reused on many sites

Examples:

- `123456`
- `admin`
- `password`

These are already in hacker databases. So they get cracked **almost instantly**.

---

7. MFA (Multi-Factor Authentication) and its importance

MFA means **more than one way to prove your identity**.

Examples:

- Password + OTP
- Password + fingerprint
- Password + authenticator app

Even if the password is stolen, **the attacker still cannot login**.

MFA adds a **second lock** to your account

---

8. Recommendations for strong authentication

- Use long passwords (12+ characters)
- Mix:
    - Uppercase ○ Lowercase ○

    - Numbers ○
    - Symbols
- Never reuse passwords
- Use a password manager
- Enable MFA everywhere possible
- Avoid common words and names
