**GOLDMAN SACHS : SOFTWARE ENGINEERING  
SIMULATION**

Name : Soumik Ghosh  
 B-Tech Final Year Student  
 CSE ’25   
 KIIT deemed to be University  
 Bhubaneswar.

**The passwords provided in the password dump file and their respective plaintext after decoding are provided below :**

**Hash Type Result**

e10adc3949ba59abbe56e057f20f883e md5 123456

25f9e794323b453885f5181f1b624d0b md5 123456789

d8578edf8458ce06fbc5bb76a58c5ca4 md5 qwerty

5f4dcc3b5aa765d61d8327deb882cf99 md5 password

96e79218965eb72c92a549dd5a330112 md5 111111

25d55ad283aa400af464c76d713c07ad md5 1234567890

e99a18c428cb38d5f260853678922e03 md5 abc123

fcea920f7412b5da7be0cf42b8c93759 md5 1234567

7c6a180b36896a0a8c02787eeafb0e4c md5 password1

6c569aabbf7775ef8fc570e228c16b98 md5 password!

3f230640b78d7e71ac5514e57935eb69 md5 qazxsw

917eb5e9d6d6bca820922a0c6f7cc28b md5 Pa$$word1

f6a0cb102c62879d397b12b62c092c06 md5 bluered

16ced47d3fc931483e24933665cded6d: md5 4f72616e6f6c696f31393934

1f5c5683982d7c3814d4d9e6d749b21e: md5 537075666679666665743132

8d763385e0476ae208f21bc63956f748: md5 6d6f6f6469653030

9b3b269ad0a208090309f091b3aba9db: md5 466c616d65736272696132303031

defebde7b6ab6f24d5824682a16c3ae4: md5 6e41626f782131

bdda5f03128bcbdfa78d8934529048cf: md5 42616e6461313173

**In most of the cases the hashing algorithm used is the MD5 hashing Algorithm.**

**The MD5 hashing algorithm provides a low level security due to a lot of technical issues in it. Some of them are mentioned below :**

**1. Lack of Salting :** The provided codes do not involve a salt. The salt is a supplementary data added to the input, to ensure that the input does not produce the same hash output at all times. Without salting, identical inputs produce the same identical hash outputs which in turn makes it vulnerable and susceptible to get cracked by attackers.

**2. Fast Computation :** MD5 is a computationally fast hashing technique that in turn makes it easy for brute force attackers to get through the hash functions by applying various permutations and combinations to decode the same.

**3. Rainbow Tables :** The availability of Rainbow Tables have made it even easier to reverse the hash functions and get access to crack the passwords easily. The MD5 too is very susceptible to this table .

**4. Hash Collision :** This MD5 Algorithm sometimes for two different inputs produce a same hash output thus leading to collision issues for the same.

**Controls to be implemented to make cracking even harder in the event of a password database leak are mentioned as follows :**

**1. Using of strong hashing algorithms:** The MD5 hashing algorithm now has outdated and due to its underlying issues it is not in use , instead algorithms like

bcrypt, scrypt and Argon2 are better as well as complex algorithms that make brute force attackers unable to carry out attacks.

**2. Using of Salt and Pepper :** Salting is a method to preserve the uniqueness of the hash outputs for similar inputs since it produces different hash outputs each time making it more secure, whereas the Pepper is a method where a secret code is added to the input before the hashing take place and it is hard coded into the machine itself.

This makes cracking passwords difficult.

**3. Limit Attempts:** This will ensure that after a certain no of failed login attempts the account gets auto locked and any unnecessary foreign user access can be thus prevented. Use of the Captcha Technique can also help in understanding whether its a human or a computerized attempt taking place.

**4. User Education:** Educating the users on how to keep their privacy maintained and their digital accounts safe by enforcing certain norms like :

i. Setting the minimum length of passwords.

ii. Use of Case sensitive letters, alphanumeric characters in their passwords.

iii. Enabling the Two-Factor Authentication for accounts to ensure the privacy.

**Overview of the Organization's Password Policy** :

1. The minimum length of the password is kept at 6.

2. The password can contain only letters and digits.

3. The passwords can start with either a letter or a digit (in accordance to the codes that are provided and the respective passwords we get after decoding them).

4. The complexity of the passwords seem to be low in nature and can be easily cracked.

5. Hashing Algorithm used in this case is MD5 which is an outdated one and offers weak security.

**The changes that can be implemented in the Password Policy for the Organization are mentioned below :**

1. The minimum length of the password can be kept at 8 or 10;

2. The password should also contain alphanumeric and special characters along with letters and digits;

3. The password should start only with a letter, not a digit or a special character;

4. The password should have a certain limit of both upper and lower case characters present in the same;

5. Advice the users to increase the complexity of the passwords for their own betterment.

6. Enabling two factor authentication by setting back up codes and passwords by linking a secondary account in order to recover back the original account in case of security breach, unauthorized access or forgetting of passwords for the accounts.