Crack leaked password database

Respected Sir/Ma'am,

After the study, it was found that Message Digest Algorithm-5 (MD-5), which is an outdated password hashing algorithm, is being used by the company to secure data.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication.

The attached password was based on the MD5 hashing, which is generally considered a weak hash algorithm, and it is easy to crack with the help of software like hashcat, codepunker, etc. That's why this hashing algorithm must be avoided by any firm/institution and adopt a very strong password encryption mechanism to create the password. To the best of my knowledge, I would suggest the concerned authority use the SHA-256 as the collision probability with SHA-256 is lower than with MD5.

The study reveals the following facts about the current password policy

- Minimum length for the password is set to 6.
- Users are free to use any set of characters on the keyboard, i.e. one can choose 111111, aaaaaa, or 1@&#Hg

There are a few suggestions that can be implemented to strengthen security:

- Minimum length for the password can be increased to 8.
- Minimum of one Capital letter is required.
- Minimum of one small letter is required.
- Minimum of one numeric digit is required.
- Minimum of one special character is required.
- Password can be changed frequently.
- The same password must be avoided.
- General information like name, date of birth, birthplace, firm name, etc should not be included in the password.

Respectfully,

Vageesh Tiwari

Indian Institute of Technology, Kharagpur

Security Password	Algorithm Used	Cracked Password
experthead:e10adc3949ba59abbe56e057f20f883e	MD5	**123456**
interestec:25f9e794323b453885f5181f1b624d0b	MD5	**123456789**
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4	MD5	**qwerty**
reallychel:5f4dcc3b5aa765d61d8327deb882cf99	MD5	**password**
simmson56:96e79218965eb72c92a549dd5a330112	MD5	**111111**
bookma:25d55ad283aa400af464c76d713c07ad	MD5	**12345678**
popularkiya7:e99a18c428cb38d5f260853678922e03	MD5	**abc123**
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759	MD5	**1234567**
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c	MD5	**password1**
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98	MD5	**password!**
liveltekah:3f230640b78d7e71ac5514e57935eb69	MD5	**qazxsw**
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b	MD5	**Pa$$word1**
johnwick007:f6a0cb102c62879d397b12b62c092c06	MD5	**bluered**