Dear Sir / Mam,

I try to crack all the leaked hashes and find that all the given hashes have been generated using the Message Digest (MD) algorithm. This MD5 algorithm divides the message into blocks of 512 bits and creates a 128 bit digest(typically, 32 Hexadecimal digits).

Since all those passwords are very weak, it is easy to crack those with HashCat or other online tools within seconds. This memo is to conclude all my findings and suggestions for improvement in your password creation policy.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication. But my suggestion is to use the SHA-256 algorithm instead of MD5, due to some reason that are,

- The output size is twice longer and the probability of collisions is lower
- A major problem of the MD5 is that it is very fast. This means that hackers can find their way into the system by trying many password possibilities. This implies that with the MD5, brute force attacks are faster than SHA-256.
- There are few reports that successful attacks on MD5 are greater than SHA-256.

Now the question arises, is there any additional process to make the hashing more secure. Then, the answer is yes and that process of making hashing more stronger & tougher to crack is salting. In salting we add some random strings in the password and then hashed it. In this method if data is leaked then without salt string hacker can not do anything with users data.

Some password policies for preventing data breach due to password decryption are.

- Standardize Password Length and Combinations (At Least 10 words in password).
- Mandatory at least one special character, number and capital letter in password.
- Avoid common words and character combinations in your password.
- Don’t reuse your passwords.
- Don’t let users include their name, address, date of birth and other important & public information while creating a password.
- Companies can also generate random and strong passwords for users.
- Need to periodically reset your password within limited days.
- Provide multi-factor authentication to strengthen power on the user side.
- Atlast, random passwords are the strongest.

These are all my views on the password hashing and updated password policies ,if readers find any useful information then my pleasure.

Regards,
Aagam Jain
B.Tech Computer Science
UIET CSJM University Kanpur

Cracked Passwords:

	Hash	Hashing Algo	Hashing Decrypt
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
flamesbria2001:	9b3b269ad0a208090309f091b3aba9db	MD5	Flamesbria2001
oranolio:	16ced47d3fc931483e24933665cded6d	MD5	Oranolio1994
spuffyffet:	1f5c5683982d7c3814d4d9e6d749b21e	MD5	Spuffyffet12
moodie:	8d763385e0476ae208f21bc63956f748	MD5	moodie00
nabox:	defebde7b6ab6f24d5824682a16c3ae4	MD5	nAbox!1
bandalls:	bdda5f03128bcbdfa78d8934529048cf	MD5	Banda11s