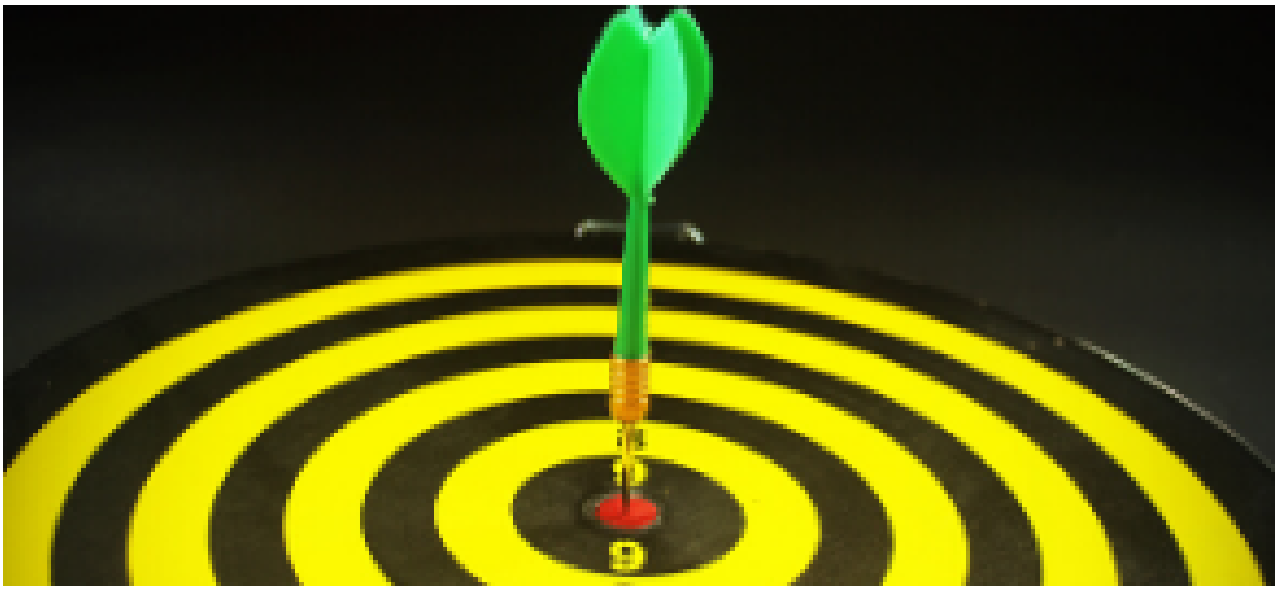
How MD5 Decryption Works?

infosecscout.com/how-md5-decryption-works

Patrick Fromaget



MD5 stands for “Message Digest 5 algorithm” and is a well-known cryptographic hash function.
They designed this function to make it impossible to decrypt, but today, it’s not yet the case …
With the growth of computing and storage through years, we can now use these tools to decrypt a lot of MD5 hash.

As there is no reverse function to decrypt a MD5 hash, the best solutions are to use techniques like brute-force or dictionary attacks. In both case, the idea is to hash a huge number of words into MD5, and try to find a match.

In this post, I’ll give you a short reminder about the MD5 hashing algorithm.
And then we’ll see how to use both methods to try to decrypt a MD5 hash.

How to encrypt a word into a MD5 hash

Without going into details, I just want to remind you the basics of MD5 encryption.

What an MD5 looks like?

An **MD5 hash is a string of 32 characters**, in hexadecimal.
Hexadecimal has only 16 characters possible: 0123456789abcdef.

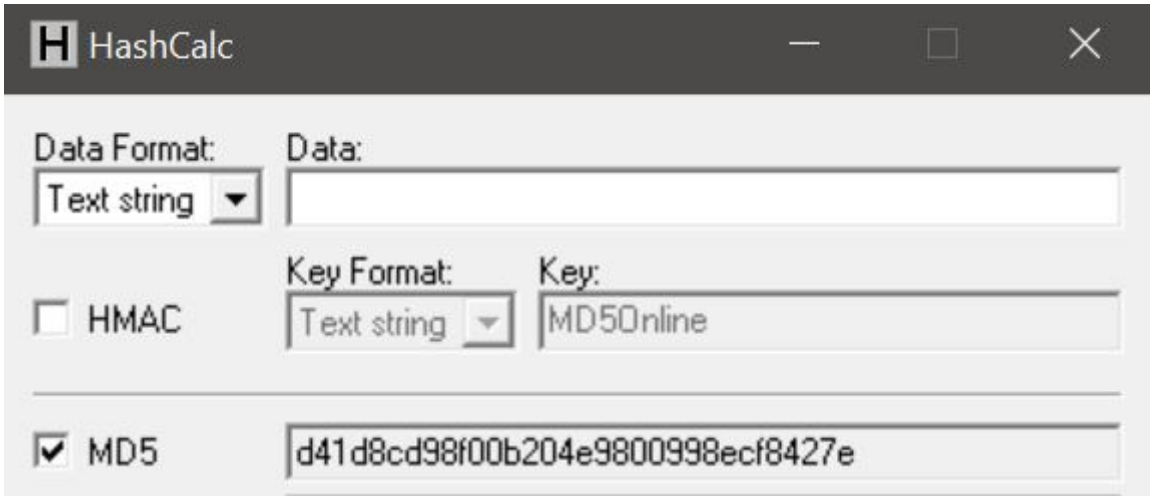
Here is an example of a MD5 hash: **d49019c7a78cdaac54250ac56d0eda8a**.

Master Ethical Hacking Skills!
Join the Complete Ethical Hacking Course Bundle and step into the world of cybersecurity.
Learn to think like a hacker and protect systems with this comprehensive course.
If you have a hash with other characters, or longer, it's not an MD5.
For example, SHA1 is a similar cryptographic algorithm with 40 characters.

How to generate a MD5 hash

The idea here is not to give you the code to generate an MD5 as it's pretty unreadable. But you need to know that there are multiple ways to generate an MD5 hash.

- **In the code**: with many languages (probably all of them), there is a function allowing you to turn a word into a MD5 hash.
  For example, in PHP, you have the function md5("string") to encrypt a word.
  This is often used to encrypt passwords into a database.
- **With a software**: You can install a software on your computer to encrypt a word into an MD5 hash.
  For example, on Windows, you can use HashCalc to encrypt a word:



  It's also working to generate MD5 file checksum.
- **Online**: And obviously, as you can encrypt a MD5 string in the code, you'll find many tools on the Internet to generate an MD5 hash from a word.
  On MD5Online, you can use this MD5 encryption tool for example.

MD5 weakness

For a human being, **this algorithm seems powerful**.
As with 32 characters having 16 possibilities, it gives
us 1,208,925,819,614,629,174,706,176 chances before to guess the word!

But **the main weakness is not directly the algorithm**, but the human password choices.
As you'll see in the next part, we'll not try every possibility.
But only the possible one, depending on the situation.

For example, if you are looking for a password hash, it's probably not longer than 10 characters.
Maybe without special characters or uppercase letters.
And finally, it may contain personal information about the user (like a child first name, the company name, the birthdate, …).
So technically, it's a way less possibilities.

There are other weaknesses in the encryption algorithm that let us believe that MD5 is not safe at all.
But for the moment, there is no evidence, so move on.

MD5 decryption with two methods

Now that you know how an MD5 can be generated, and why it's not so safe, we can move to the decryption parts.
How does it work? We'll see the two main used methods to decrypt an MD5 hash.

Brute force a MD5

The first way to decrypt an MD5 hash is to brute force it.
A brute force attacks goal is to try many words, convert them into MD5, and check if the MD5 hash is corresponding to what we are looking for.

Example

Let's take a basic example. You have this hash: 8277e0910d750195b448797616e091ad.
You don't know what it is, but you need to find it.
If you have absolutely no idea of what it is, **you'll try every possibility**.
It's quite the same thing as if you try to unlock a 3 digits lock, you'll try any numbers from 000 to 999.

So in my example, I'll try:

- **a**: If I encrypt it into a MD5 hash I get: 0cc175b9c0f1b6a831c399e269772661.
  It's not the MD5 I'm looking for.
- **b** => 92eb5ffee6ae2fec3ad71c777531578f.
  Not this one.
- **c** =>4a8a08f09d37b73795649038408b5f33.
  Nope.

- **d** => 8277e0910d750195b448797616e091ad.
  It's a match, we found the corresponding MD5!

It's a very basic example to explain you, in real life you'll try a thousand of words each second, and you may never find the corresponding word.

In real life

As I told you previously, in real life you'll probably not start like this.
You may already know that the password can't be shorter than 8 characters, so you can start at aaaaaaaa, previous words are not possible.
And you may also know some possible combinations.

Most of the time, **hackers will build a list of all easy possibilities**.
Like the child's names, the child first name + X digits, birthdates, …
They compile of these possibilities in a file called a dictionary.

Even if the dictionary contains 100 million words, it is always easier than trying all the possible words.

How to brute force an MD5 hash?

As you probably guess it, you'll not try 100 million words manually.
There are many free tools you can use to brute force an MD5 hash.

The goal of this post is not to teach you how to use them, but you'll find some useful information on their websites.
Here are three tools you can try to **brute force an MD5 password**:

- John the Ripper
  One of the most popular because it exists for many years.
  It's available for any operating system.
- Hydra
  Hydra is another fast tool to decrypt password.
  It's not only doing brute force attack but also various types of attacks.
- RainbowCrack
  This is the last tool example I give you.
  It's a tool using a dictionary attack, they provide many rainbow tables you can download to use the software, but you can also build yours.

MD5 database

The second method, and the easiest one is to use an MD5 database to find the corresponding word.

What is an MD5 database?

An MD5 database is like the dictionary we talk about previously.
You can create **a file with the word and the corresponding MD5 hash**.

Here is a short example:

```
a:0cc175b9c0f1b6a831c399e269772661
b:92eb5ffee6ae2fec3ad71c777531578f
c:4a8a08f09d37b73795649038408b5f33
d:8277e0910d750195b448797616e091ad
```

You can store many words like this.
And the bigger the table is, the more likely you are to find the word for any MD5 hash.

Master Ethical Hacking Skills!
Join the Complete Ethical Hacking Course Bundle and step into the world of cybersecurity.
Learn to think like a hacker and protect systems with this comprehensive course.

How to use it?

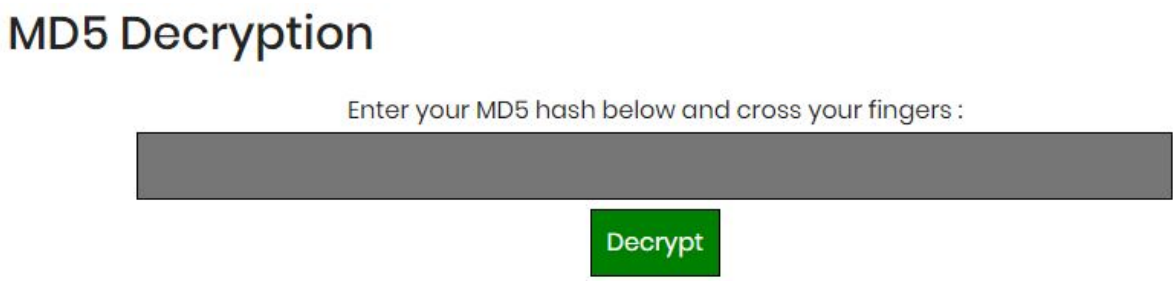
Basically, you can use with a search function.
If you store this in a text file, you can use the search function of any editor to look for the MD5.
But for bigger tables this is not possible.

Most of the time you'll **have a software making requests in this table** to find the corresponding word.
On M5Online.org, we have several databases, on several servers, so it's not possible to find an MD5 hash with a simple CTRL+F 🙂

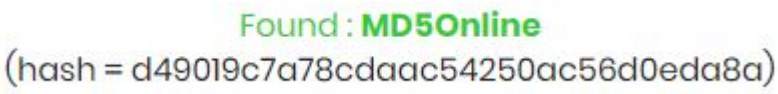
How to decrypt a MD5 hash on MD5Online?

Making a request in our giant database is free, and you can do this online.
To do this, follow this procedure:

- Access the MD5 decrypt page by clicking on the link.
- You'll get a form like this:



- Enter your MD5 hash in the field and hit "Decrypt".
  For the example, you can use this one: d49019c7a78cdaac54250ac56d0eda8a.
- After a few seconds, you'll get a result, like this one for the sample MD5 hash:



- If there is no result, you can give an email address to receive a notification when the MD5 hash will be decrypted.

It will not work for any word, but with over 1,154 billion words in the database (and growing), there is a big chance that weak passwords will be found.

Related questions

Is it possible to have the same MD5 hash for two words? Yes, it's possible, there is no uniqueness in the MD5 algorithm. But the chances are low to have this kind of situation.

What's the chance of finding a password in the MD5Online database? They are pretty high. For a short word like a password of 5 to 10 characters, there is a good chance you find it, even with uppercase and special characters. Globally, the success rate on MD5Online.org is over 50%.

Conclusion

That's it, you now know how MD5 decryption works, and how to use it with two different methods.
I highly recommend starting with the MD5 database from MD5Onine before trying anything else.
You'll save a lot of time by doing this.

If you have many words to decrypt, don't forget that we have some advanced plans with unlimited use of the tools, and an API to automate your work.

Whenever you're ready for more security, here are things you should think about: