How to Decrypt MD5 in JavaScript? (Solution with examples)

infosecscout.com/decrypt-md5-in-javascript

Patrick Fromaget

Cracking MD5 hashes is interesting for many people, and if you are programming in JavaScript you are at the perfect place. In this article, you'll learn how to use MD5 in JavaScript and also how to decrypt MD5 hashes.

The MD5 hash function works in one way only, there is no reverse function, whatever the language used. In JavaScript, it's possible to hash strings to get an MD5 digest, but there is no direct method to get back the original word from a MD5 hash.

The only way to crack an MD5 in JavaScript is to used advanced techniques, like the one I will show you at the end of this article. But first, let do a quick reminder about the MD5 algorithm.

By the way, if you are interested in how MD5 decryption really works, I highly encourage you to take a look at my e-book "The Secrets of MD5 Decryption"here. It explains everything you need to know, going directly to the point with practical examples you can test on your computer. You don't need any hardware to get started, just a few tips I give in this book.

Master Linux Commands
Your essential Linux handbook
Want to level up your Linux skills? Here is the perfect solution to become efficient on Linux. **20% off today!**

Download now

What is the MD5 algorithm?

How MD5 encryption works?

Hide your IP address and location with a free VPN:
Try it for free now, with advanced security features.
2900+ servers in 65 countries. It's free. Forever.
MD5 is a cryptographic algorithm that generate a string with 32 hexadecimal characters, whatever the word or text length you try to encrypt. Even large files like ISO images with gigabytes of data will be hashed to a 32 characters string.

Pseudo-code example:
```
MD5("MD5Online") = d49019c7a78cdaac54250ac56d0eda8a
```

This information provides the following algorithm results:

The output is always 32 characters long, but you can hash anything in 32 characters.
So, the MD5 algorithm output is not unique. Two word or files can have the same MD5 hash (as explained in this article).
Given this information, it's not possible to reverse a hash to the original word.

What is MD5 decryption?

When talking about the MD5 algorithm, "decryption" is the wrong word. There is no reverse function, so there is no way to "decrypt" a MD5 hash. However, there are several techniques that can be used to crack a MD5 hash and recover the original word.

Indeed, the MD5 algorithm has a weakness we can exploit, each time you create a MD5 hash of a word, you get the same result. As this algorithm was the most used in the world a few decades ago, many databases exists with the corresponding word for each MD5 they know.

So, there is no decryption algorithm for MD5, but there is a solution.
For example, you now know that the MD5 hash from "MD5Online" is d49019c7a78cdaac54250ac56d0eda8a.
If someone is looking for the word corresponding to this hash, there is a good chance that "MD5Online" was the original password.

That basically how the website MD5Online.org works. With a giant database of over a trillion hashes stored with their clear text equivalent, there is a high chance to crack the most common words and passwords.

How to Encrypt a Password with MD5 in JavaScript?

In JavaScript, there is no native function to use the MD5 algorithm and hash a word. However, some libraries can be used to add the md5() function and easily use it to encrypt words in MD5.

For example, you can use the one from blueimp, available here on GitHub.
You can either install with NPM by using the following command:
`npm install blueimp-md5`
Or just download and import the MD5 JavaScript file in your script:
`<script src="md5.js"></script>`

Once done using it should be pretty easy, as the md5 function will now be available directly, for example:

```
<script src="md5.js"></script>
<script>
        var hash = md5("MD5Online");
        alert(hash);
</script>
```

This short code should display the MD5 hash corresponding to MD5Online in a popup message.
Obviously, you can adapt this minimal code to your goals and use the md5 function in a smarter way.

For example, if you have passwords stored somewhere in MD5, you can just compare the MD5 hash of the typed password with the store one. You don't necessarily need to decrypt the stored one to confirm the correct authentication.

It should be something like this:

```
if(md5(typed_password) == stored_password) {
   //authentication confirmed
}
```

But if that wasn't your original question, let's see now how to crack the MD5 hash you have.

How to Decrypt a MD5 hash in JavaScript?

There is no native method to decrypt a MD5 hash in JavaScript, but MD5Online has an API that can be used in JavaScript to try to crack a MD5 hash and recover the original word.

Become a Cyber Security Expert!:
Enroll in the Complete Cyber Security Course now, and master online safety.
Learn to defeat hackers, protect privacy, and stay anonymous with over 50 hours of on-demand video.
This API will look in the huge database I introduced previously, and also use other secret techniques to give you the best chance to crack MD5 hashes (the success rate was 87% last month).

Anyway, here is how to use this API in JavaScript. A documentation is available, but basically, it's just a request to a specific URL, including all the parameters in GET (like the API key, the MD5 hash and a few other options).
By the way, this is a paid service, you'll need a few credits to test it (more details here).

Here is a basic example:

```
var key = "YOUR_API_KEY";
var hash = "d49019c7a78cdaac54250ac56d0eda8a";
var url = "https://www.md5online.org/api.php?d=1&p="+key+"&h="+hash;

const http = new XMLHttpRequest();
http.open("GET", url);
http.send();
http.onreadystatechange=function()
{
  if (http.readyState==4 && http.status==200)
  {
    alert(http.responseText);
  }
}
```

If you have a decent level in JavaScript, it should be pretty easy for you. We are just using XMLHttpRequest like for an Ajax request. If it works correctly on your side, you can then start from there and change the code to do whatever you want. For example, get your MD5 hashes from a specific source and then call the API for each hash in a loop.

Conclusion

That's it, you now know how to use MD5 hashes in JavaScript. You know how to generate MD5 hashes but also the only way to crack them.

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

- **Break free from Gmail**: You should be able to choose what happens to your data. With Proton, only you can read your emails. Get private email.

- **Protect yourself online**: Use a high-speed Swiss VPN that safeguards your privacy. Open-source, no activity logs. Get Proton VPN risk-free.

- **Master Linux commands**: A sure method to learn (and remember) Linux commands. Useful ones only, one at a time, with clear explanations. Download the e-book.