# Hacker Tools: Ciphey – Automatic decryption, decoding & cracking

BY ANNA HAMMOND · AUGUST 11, 2021 · LAST UPDATED ON MARCH 6, 2025

*Have you ever come across an encoded string, hash, or encrypted message and wondered: "What type of encoding is this?"? Then Ciphey is the tool for you!*

## What is Ciphey?

"What type of encryption is this?", "What hashing algorithm produced this hash?", "What cipher is being used?". The answer to those questions, that's what Ciphey is.

> **"Ciphey aims to be a tool to automate a lot of decryptions & decodings such as multiple base encodings, classical ciphers, hashes or more advanced cryptography.**
>
> **Ciphey README.md"**

That quote doesn't do Ciphey enough justice. It all starts with your input. At that point, neither you nor the tool knows anything about it. Firstly, an AI-powered module named AuSearch will start performing a cipher detection to approximate what something is encrypted with. Using a language checker interface, it can start to detect when a decryption step gets your input closer to plaintext. It will then recursively keep on trying to find the correct decryption method to get you closer and closer to the plaintext message.

That may sound very complicated, and it is, but luckily you don't need to worry about that. All you need to do is run the tool and that couldn't be simpler. Just look at this GIF from the Ciphey documentation. In a matter of seconds, the tool found that if you reverse the string, then perform a vigenere cipher with key nn, reverse again, utf8 decode, base64 decode, utf8 decode, base32 decode, utf8 decode, and then once more base64 decode, you get the plaintext.

The example above will obviously never occur in real-life situations, however, it is clear that a tool this powerful could come in handy in various situations!

## How do I install it?

Installing Ciphey is peanuts! It couldn't have been made easier and the documentation is amazing. Visit the repository for extended information or check out the quick summary on ways to install below.

- Python: **`python3 -m pip install ciphey --upgrade`**
- Docker: **`docker run -it --rm remnux/ciphey`**
- MacPorts: **`sudo port install ciphey`**
- Homebrew: **`brew install ciphey`**

# How do I use it?

The installation was a breeze, so is using it. In essence, you only need to remember 2 commands.

- **ciphey -f file**
- **ciphey -t string**

Using these commands, we can run ciphey on files and strings of any size!

My suggestion is to add this tool to your list of things to do when you encounter a string or character sequence you don't know!

# What can it do?

Here comes the good stuff: the features of this tool

- Supports over 30 cipher & encodings: Caesar Cipher, ASCII shift, Vigenère Cipher, Affine Cipher, XOR, base64, base32, baseXX, braille, morse & many more!
- Multilanguage support.
- C++ core for lightning fast execution.
- Customizable.
- Not opinionated. Base64, for example, has many different syntaxes. Instead of just implementing one, Ciphey checks all of them!
- Amazing documentation.

If this list of features does not convince you yet, keep this in mind. This tool has been designed very carefully and has a very robust architecture. This means that adding new ciphers, checkers, hashes, and encryptions is very simple. More cool stuff is to come as time goes on so be sure to keep an eye on this amazing tool!

# Conclusion

Ciphey is a powerful tool that will help you understand the meaning and origin of strings you may come across on your bug bounty journey.

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out all the previous Hacker Tools articles, such as the last one on NoSQLMap.

---

Did you know that there is a video accompanying this article? Check out the playlist!

**REQUEST A DEMO**

intigriti.com/demo

**VISIT THE WEBSITE**

intigriti.com

**GET IN TOUCH**

hello@intigriti.com