



UNIVERSITY *of* NICOSIA

Session 2

How to use an online hash converter: step-by-step guide

DFIN 511: Introduction to Digital Currencies

Session 1: Objectives

The purpose of this step-by-step guide is to demonstrate how to use an online hash converter, and to learn some interesting properties of hashes.

The concept of using an online hash converter is introduced in this week's learning material.

Several online hash converters exist. Let's take a look at <https://hash.online-convert.com/> indicated in the slides.



How to use an online hash converter: step-by-step guide

Go to <https://hash.online-convert.com/>

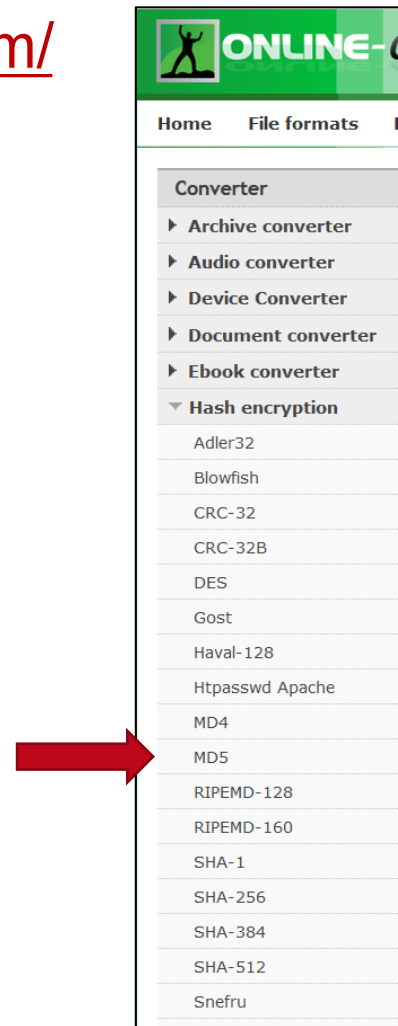
The screenshot shows the homepage of the hash.online-convert.com website. The header features the site logo, a tagline 'Convert media free, fast and online. No software installation needed.', and 'Login' and 'Register' buttons. A navigation bar includes links for 'Home', 'File formats', 'Blog', and 'Developers', along with a language selector set to 'EN' and a 'Menu' dropdown. A left sidebar lists various conversion tools under the 'Converter' category, with 'Hash encryption' expanded to show options like Adler32, Blowfish, CRC-32, and SHA-1. The main content area is titled 'Convert hashes online' and includes a search bar with suggestions like 'md5 decrypter', 'sha1 hash encoder', and 'convert to mp3'. Below this is an advertisement for '2020 Password Managers' with an 'OPEN' button. The right sidebar contains social media sharing options for 'Bookmark Hash encryption' and 'Like 112K' buttons for Facebook, Twitter, and LinkedIn. The footer of the main content area lists several online tools: 'Adler32 online generator', 'Create a Blowfish hash with salt', 'CRC-32 online checksum calculator', and 'Calculate CRC-32B checksums online', each with a 'Read more...' link.

How to use an online hash converter: step-by-step guide

Go to <https://hash.online-convert.com/>

Many hashing algorithms exist

- You may wish to observe that a variety of hashing algorithms exist.
- Let's explore a simple hashing algorithm such as MD5.



How to use an online hash converter: step-by-step guide

Go to <https://hash.online-convert.com/>

- Input the word: Bitcoin
- Click 'Convert file'
- MD5 hash: d023e...5089

Conversion Completed

Your hash has been successfully generated.

hex: d023ec040f79f1a9b2ac960b43785089

HEX: D023EC040F79F1A9B2AC960B43785089

Upload and generate a MD5 checksum of a file:


No file selected.


Or enter the text you want to convert to a MD5 hash:

Bitcoin

Or enter URL of the file where you want to create a MD5 hash:

Or select a file from your cloud storage for a MD5 conversion:

 Choose from Dropbox

 Choose from Google Drive

Optional settings

Shared secret key used for
the HMAC variant (optional):

Save settings

Save settings as:



([Log in](#) to activate)

(by clicking you confirm that you have understand and agree to our [terms](#))

How to use an online hash converter: step-by-step guide

Now try <https://8gwifi.org/MessageDigest.jsp>

Now let's try another similar online converter

- Use the same word 'Bitcoin' and the same MD5 hashing algorithm
- Let's explore a simple hashing algorithm such as MD5.
- Observe that the same hash is generated d023e...5089

Get Message Digest Information

Input Message

Bitcoin

Choose Message Digest

MD5
md2
md4
ripemd128
sha
sha-1
sha-224
sha-256
sha-384
sha-512

Message [Bitcoin]
Algo [Digest Length 16]
Algo MD5 Base64 Encoded [0CPsBA958amvrJYLO3hQiO==]
Algo MD5 Hex Encoded [d023ec040f79f1a9b2ac960b43785089]

How to use an online hash converter: step-by-step guide

Now hash the word 'bitcoin' (lower case b)

- Go to <https://hash.online-convert.com/>
- Input the word: bitcoin (lower case b)
- Click 'Convert file'
- MD5 hash: cd5b...579a
- A completely different hash has been generated

Conversion Completed
Your hash has been successfully generated.

hex: cd5b1e4947e304476c788cd474fb579a

HEX: CD5B1E4947E304476C788CD474FB579A

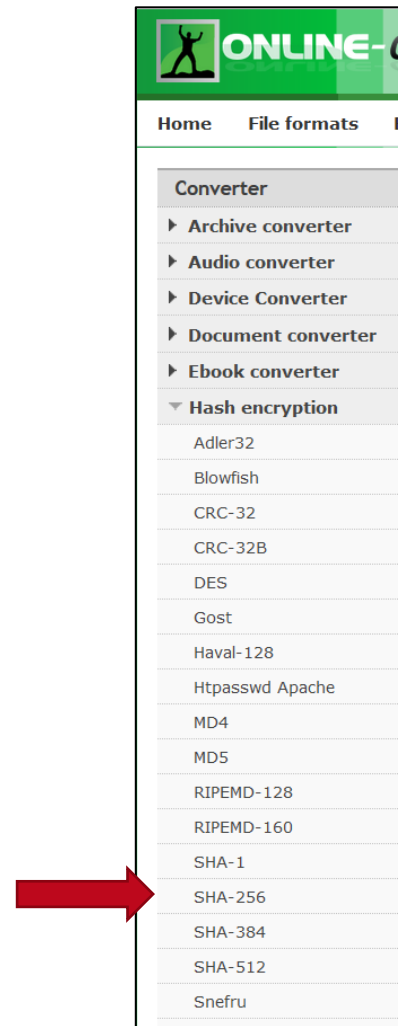
The screenshot shows the 'hash.online-convert.com' website interface. On the left, a sidebar lists various hash algorithms: Htpasswd Apache, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Snefru, Tiger-128, Tiger-160, Tiger-192, Whirlpool, Image converter, Software Converter, Video converter, and Webservice converter. A red arrow points to the 'RIPEMD-160' option. The main content area has three sections: 'Upload and generate a MD5 checksum of a file:' with a 'Browse...' button and 'No file selected.' text; 'Or enter the text you want to convert to a MD5 hash:' with a text input field containing 'bitcoin'; and 'Or enter URL of the file where you want to create a MD5 hash:' with an empty text input field. Below these is 'Or select a file from your cloud storage for a MD5 conversion:' with buttons for 'Choose from Dropbox' and 'Choose from Google Drive'. There is an 'Optional settings' section with a 'Shared secret key used for the HMAC variant (optional):' input field. A 'Save settings' section has a 'Save settings as:' label, an 'Enter a name' input field, and a '(Log in to activate)' link. At the bottom, a 'Convert file' button is shown with a red arrow pointing to it, and a note '(by clicking you confirm that you have understand and agree to our terms)'.

How to use an online hash converter: step-by-step guide

SHA-256 hashing algorithm

Let's try SHA-256, a more sophisticated hashing algorithm, also used in Bitcoin mining protocol

- Go to <https://hash.online-convert.com/>
- Select SHA-256 algorithm



How to use an online hash converter: step-by-step guide

SHA-256 hashing algorithm

- Input the word: Bitcoin
- Click 'Convert file'
- SHA-256 hash: b4056...3aa4

Conversion Completed

Your hash has been successfully generated.

hex: b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

HEX: B4056DF6691F8DC72E56302DDAD345D65FEAD3EAD9299609A826E2344EB63AA4

Upload and generate a SHA256 checksum of a file:


No file selected.

Or enter the text you want to convert to a SHA-256 hash:

Bitcoin|

Or enter URL of the file where you want to create a SHA256 hash:

Or select a file from your cloud storage for a SHA256 conversion:

 Choose from Dropbox

 Choose from Google Drive

Optional settings

Shared secret key used for the HMAC variant (optional):

Save settings

Save settings as:



([Log in](#) to activate)

(by clicking you confirm that you have understand and agree to our [terms](#))

Conclusions

Key learning points regarding hashes

- Various hashing algorithms exist
- When using the same algorithm, the same word/input will always generate the same hash
- The slightest change in the input will generate an entirely different hash
- Different inputs should never generate the same hash (collision free)
- Is difficult to guess (reverse engineer) the input value from its output/hash





UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**

Course Support: **digitalcurrency@unic.ac.cy**

IT & Live Session Support: **dl.it@unic.ac.cy**