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

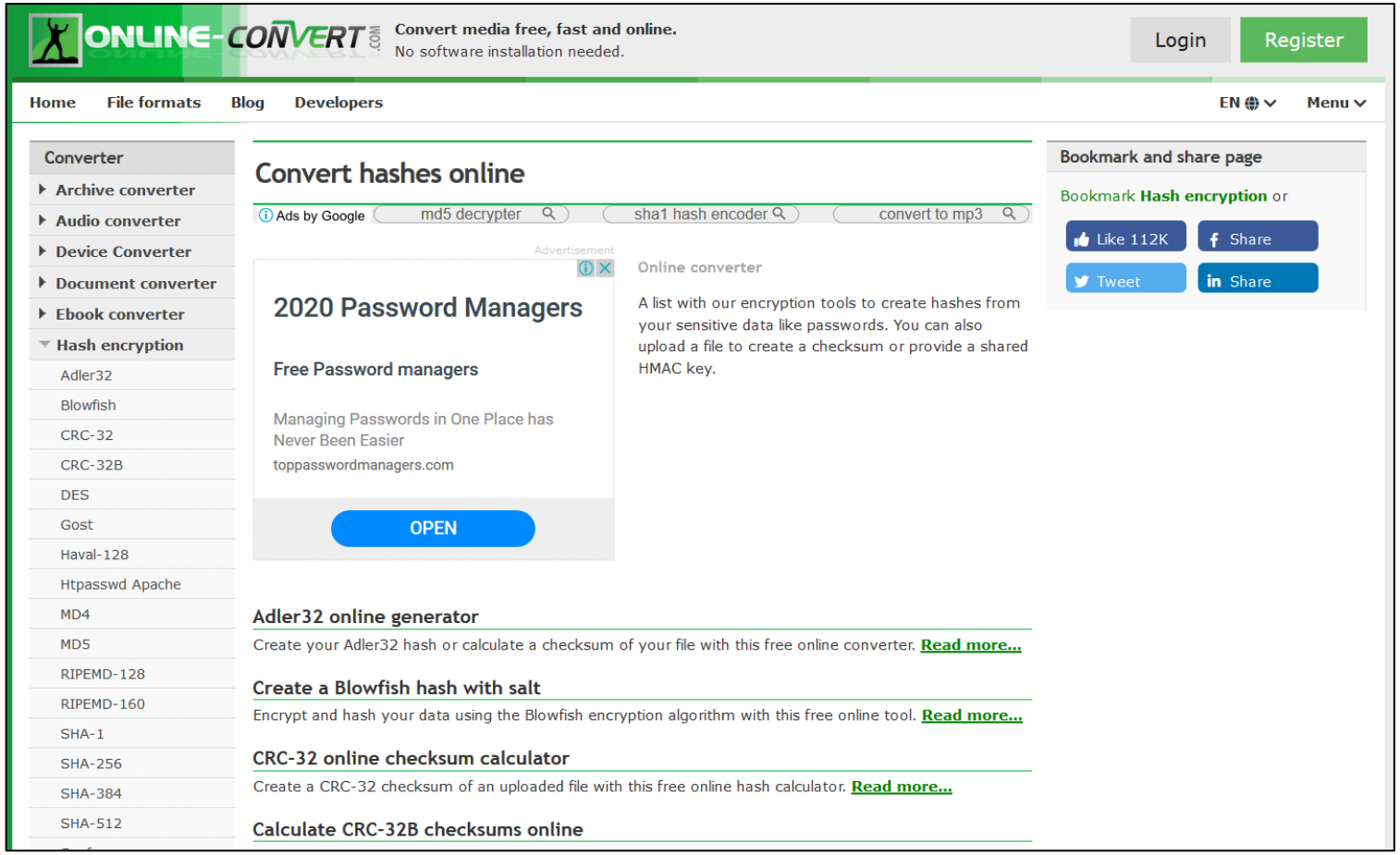
The purpose of this step-by-step guide is to demonstrate how to use an online hash converter, and to learn some interest properties of hashes.

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/

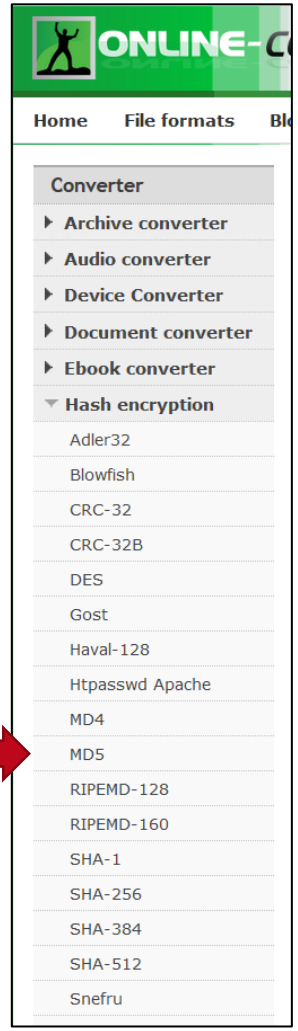


How to use an online hash converter: step-by-step guide

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

Upload and generate a MD5 checksum of a file:

Browse... 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: Enter a name (Log in to activate)

Convert file (by clicking you confirm that you have understand and agree to our terms)

Conversion Completed

Your hash has been successfully generated.

hex: d023ec040f79f1a9b2ac960b43785089

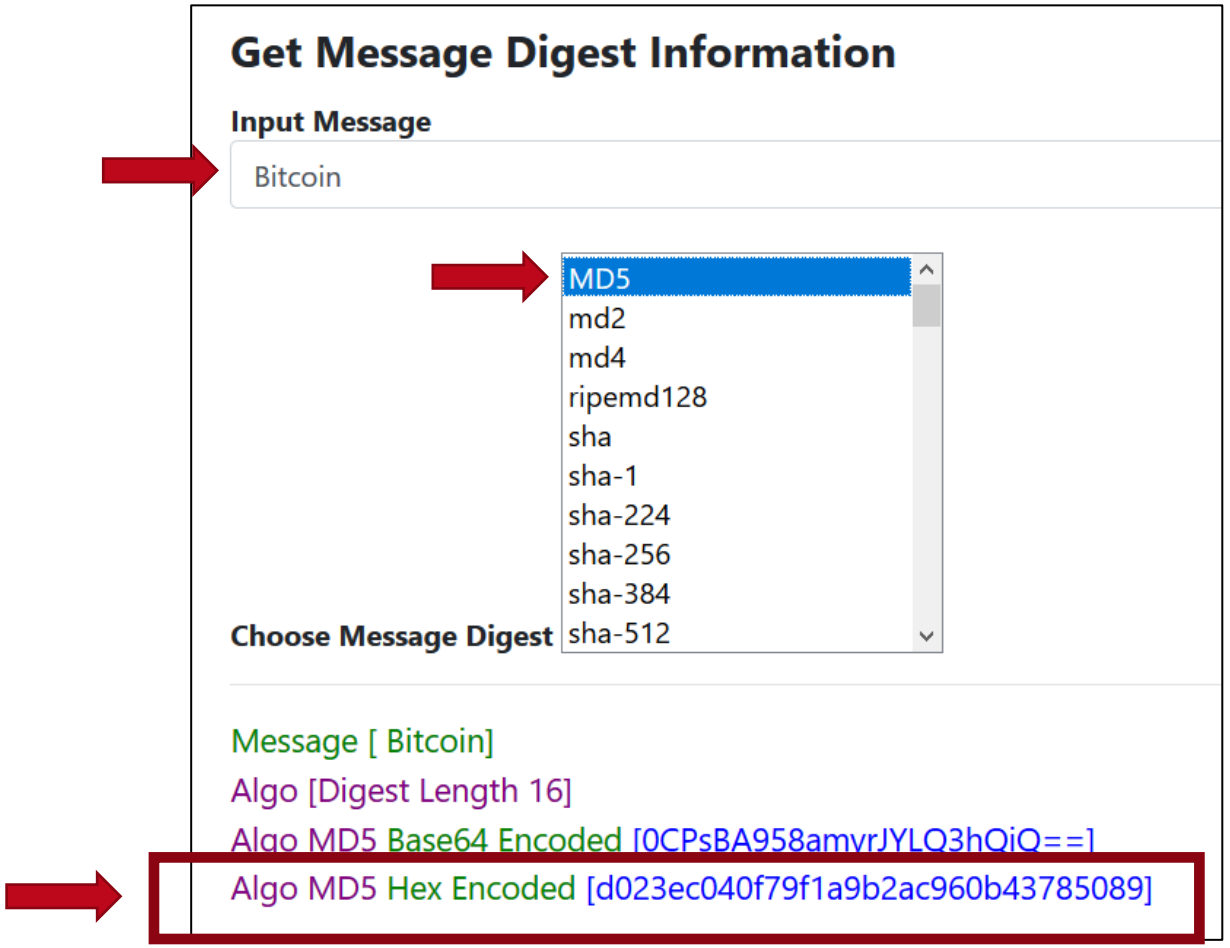
HEX: D023EC040F79F1A9B2AC960B43785089

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



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

Now hash the word ‘bitcoin’ (lower case b)

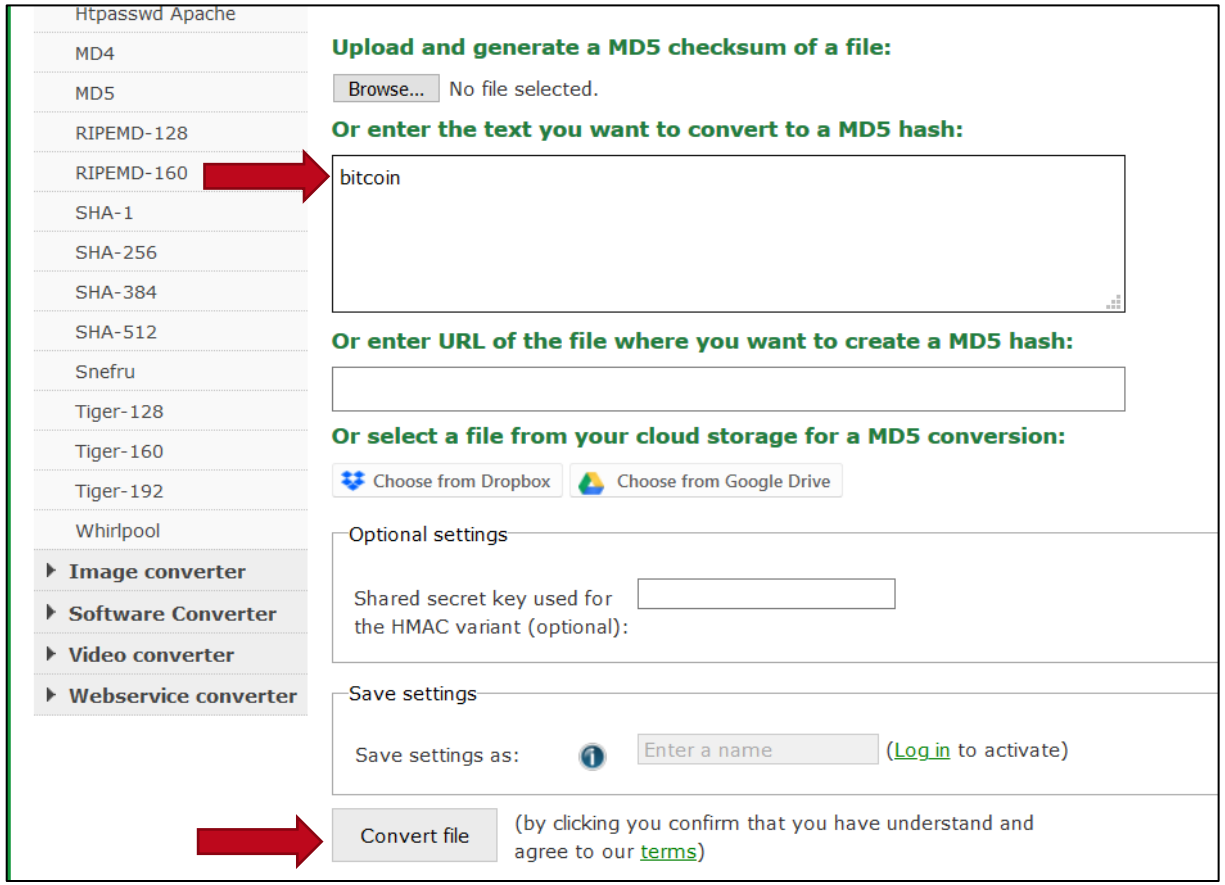
- Go to https://hash.online-convert.com/
- Input the word: bitcoin (lower case b)
- Click ‘Convert file’
- MD5 hash: cd5b…579a
- A completely different hash has been generated

Conversion Completed

Your hash has been successfully generated.

hex: cd5b1e4947e304476c788cd474fb579a

HEX: CD5B1E4947E304476C788CD474FB579A

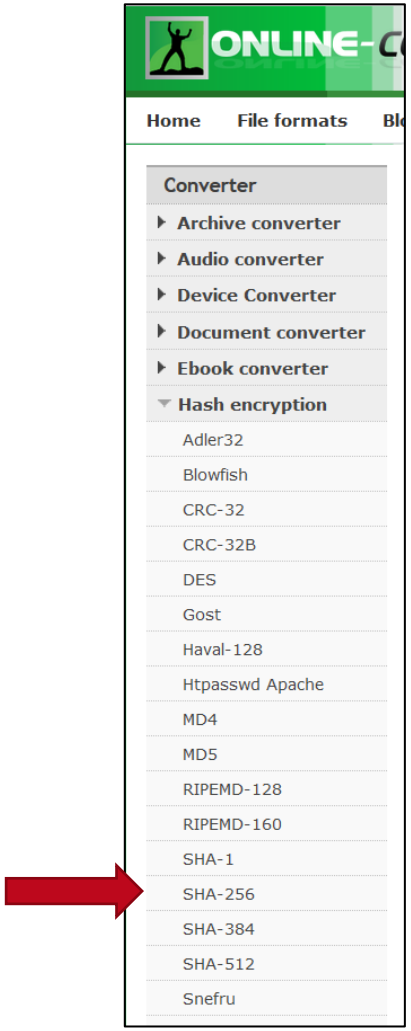


How to use an online hash converter: step-by-step guide

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

Upload and generate a SHA256 checksum of a file:

Browse... 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: Enter a name (Log in to activate)

Convert file (by clicking you confirm that you have understand and agree to our terms)

Conversion Completed

Your hash has been successfully generated.

hex: b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

HEX: B4056DF6691F8DC72E56302DDAD345D65FEAD3EAD9299609A826E2344EB63AA4

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**