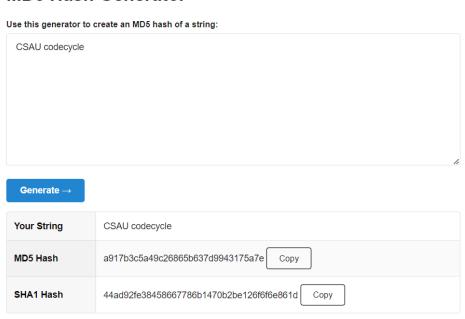
Round 1: Cryptography

Screen Captures:

SECTION 1:

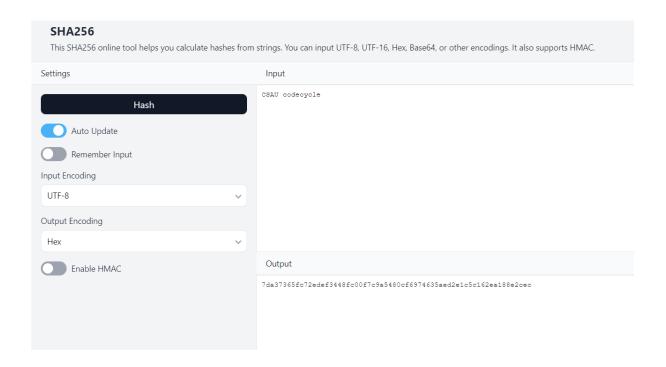
MD5 Hash Generator

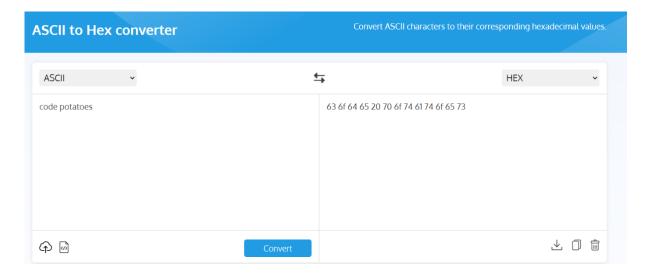


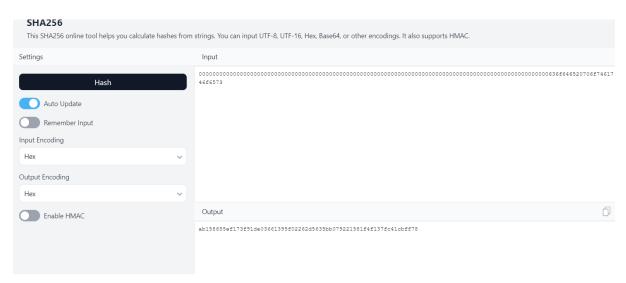
Use this generator to create an MD5 hash of a string:

A lot of people confuse the term cryptography with cryptocurrency like bitcoin. Actually cryptography is a mathematical / computer science way to secure data communication in the presence of an adversary or attacker. In short, it deals with the jargon that most of the security people use: encryption, decryption, hashing, digital signatures, digital certificates and so on. Whereas cryptocurrency is one such application of cryptography along with a consensus mechanism, peer to peer network and transactions.

Your String A lot of people confuse the term cryptography with cryptocurrency like bitcoin. Actually cryptography is a mathematical / computer science way to secure data communication in the presence of an adversary or attacker. In short, it deals with the jargon that most of the security people use: encryption, decryption, hashing, digital signatures, digital certificates and so on. Whereas cryptocurrency is one such application of cryptography along with a consensus mechanism, peer to peer network and transactions. MD5 Hash O1ac5a11a9cd6e78055e1556c305630bab0f934a Copy Copy O1ac5a11a9cd6e78055e1556c305630bab0f934a Copy







INSTALLING ZOKRATES

```
janesh@janesh-VirtualBox:/$ curl -LSfs get.zokrat.es | sh
ZoKrates: Tag: latest (0.8.8)
ZoKrates: Detected architecture: x86_64-unknown-linux-gnu
ZoKrates: Installing to: /home/janesh/.zokrates
ZoKrates: Fetching: https://github.com/ZoKrates/ZoKrates/releases/download/0.8.8/zokrates-0.8.8-x86_64-unknown-linux-.tar.gz
ZoKrates was installed successfully!
If this is the first time you're installing ZoKrates run the following:
export PATH=$PATH:/home/janesh/.zokrates/bin
janesh@janesh-VirtualBox:/$ zokrates --version
zokrates: command not found
janesh@janesh-VirtualBox:/$ export PATH=$PATH:/home/janesh/.zokrates/bin
janesh@janesh-VirtualBox:/$ zokrates --version
ZoKrates 0.8.8
janesh@janesh-VirtualBox:/$
```

sha256.zok file

```
import "hashes/sha256/512bitPacked" as sha256packed;

def main(private field a , private field b, private field c, private field d, field h0, field h1){
    field[2] h = sha256packed([a,b,c,d]);
    assert(h[0] == h0);
    assert(h[1] == h1);
    return;
}
```