

# Round 1 : Cryptography

## Screen Captures:

### SECTION 1 :

#### MD5 Hash Generator

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

CSAU codecycle

Generate →

Your String	CSAU codecycle	
MD5 Hash	a917b3c5a49c26865b637d9943175a7e	Copy
SHA1 Hash	44ad92fe38458667786b1470b2be126f6f6e861d	Copy

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.

Generate →

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	cf99c1a5e9f27a642086759508552806	Copy
SHA1 Hash	01ac5a11a9cd6e78055e1556c305630bab0f934a	Copy

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

## Settings

### Input

## Hash

CSAU codecycle

☒ Auto Update

☐ Remember Input

## Input Encoding

UTF-8

## Output Encoding

Hex

☐ Enable HMAC

## Output

7da37365fc72edef3448fc00f7c9a5480cf6974635aed2e1c5c162ea188e2cec

## Convert ASCII characters to their corresponding hexadecimal values.

ASCII



## HEX

code potatoes

63 6f 64 65 20 70 6f 74 61 74 6f 65 73

   

This SHA256 online tool helps you calculate hashes from strings. You can input UTF-8, UTF-16, Hex, Base64, or other encodings. It also supports HMAC.

## Settings

Input

Hash

[illegible]

☒ Auto Update

☐ Remember Input

## Input Encoding

Hex

## Output Encoding

Hex

☐ Enable HMAC

### Output

ab158655ef173f91de03661395f02262d5635bb079221581f4f137fc41cbff78

## 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

```
janesh@janesh-VirtualBox: /
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;
}
~
~
~
~
~
~
```