Hash Functions

A hash function maps data of arbitrary length to a unique fixed length string, called digest.

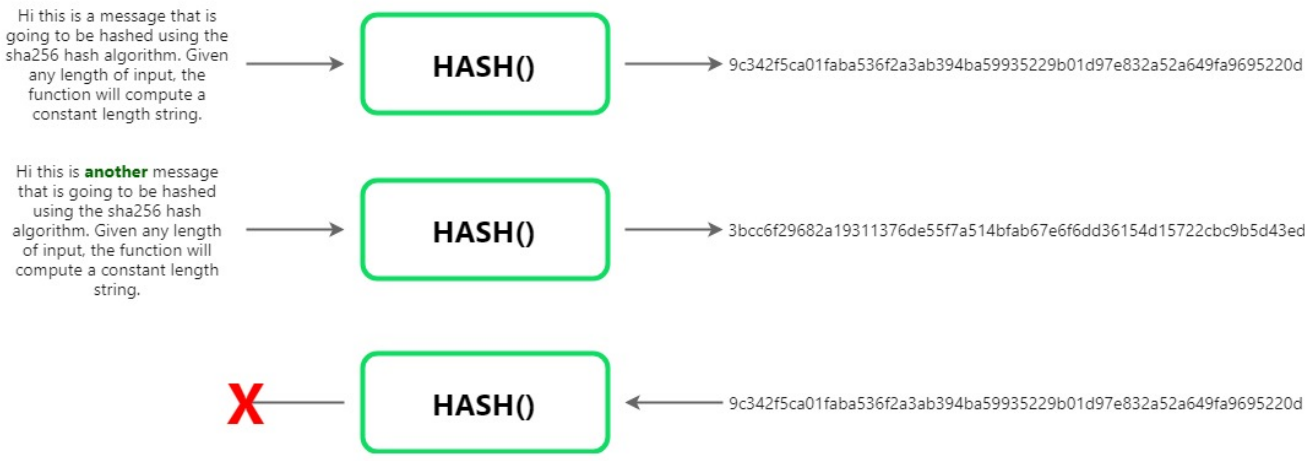
WE'LL COVER THE FOLLOWING

A hash value for a data is X is a function:

```
HASH(X) = Y
```

Such that:

- No other X' can have HASH(X') equal to Y. Its one to one mapping.
- The size of Y is fixed and the size of X can be arbitrary.
- Given Y you can not calculate X. Its a one-way function!



Hash Functions for Checking Integrity

This means that I can take a huge text file and compute its unique digest using a hash function. If I send that file and its computed hash along with it to a receiver, Bob, Bob can then recompute the hash to ensure that the content of that file were not corrupted in the transmission. When we download a file

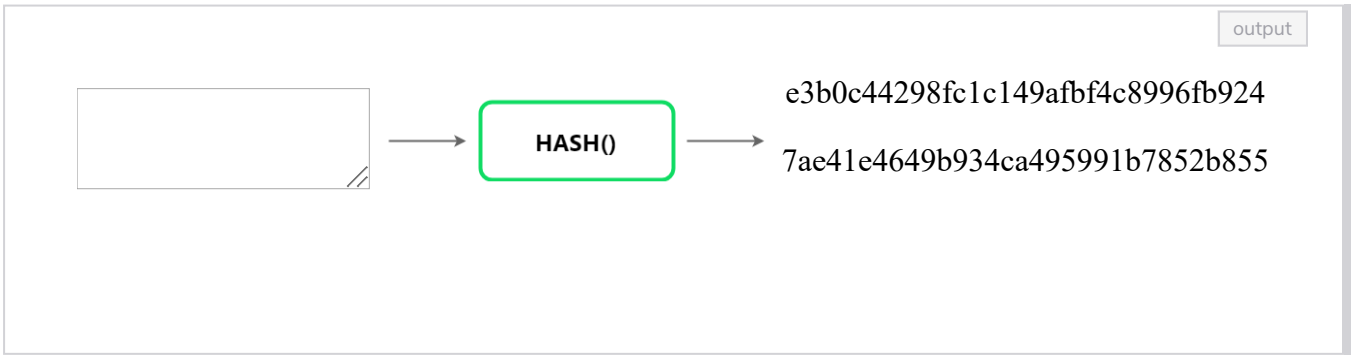
from the internet, it uses the same hash functions to verify its integrity.

SHA256 Hash Function

There are multiple standardized hash function implementations that are used, such as SHA256, which we will be using in our course.

You can find libraries that implement SHA256 hash in all technologies, so you never have to write your code for SHA256 implementation.

Here is a small Javascript widget that will calculate sha256 of any data you enter:



Test Yourself

1 Which of the following statements is true?

COMPLETED 0%

1 of 3

In the next lesson, we will discuss what Public key cryptography is.