

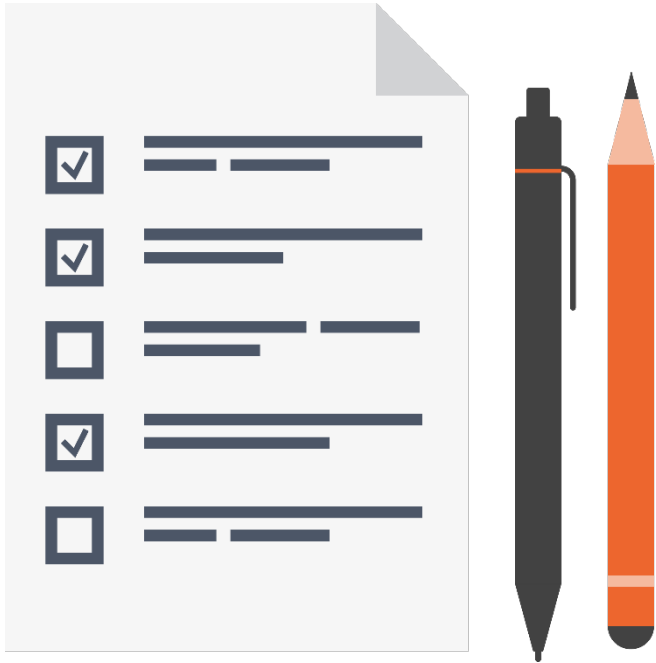
Hashing Algorithms



Stephen Haunts

@stephenhaunts | www.stephenhaunts.com

Overview



- What is Hashing?
- MD5
- Secure Hash (SHA) Family
- Hashed Message Authentication Codes (HMAC)

What Is Hashing?

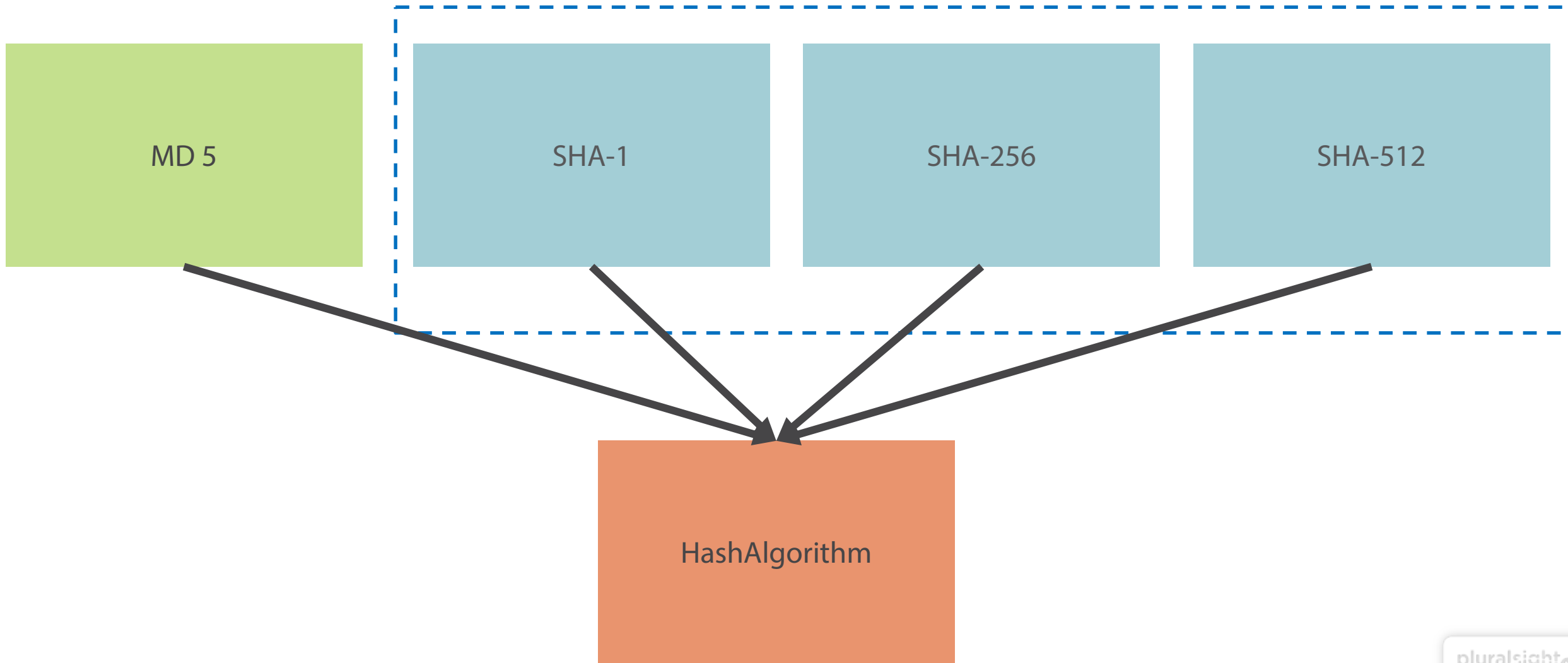


- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash

What Is Hashing?



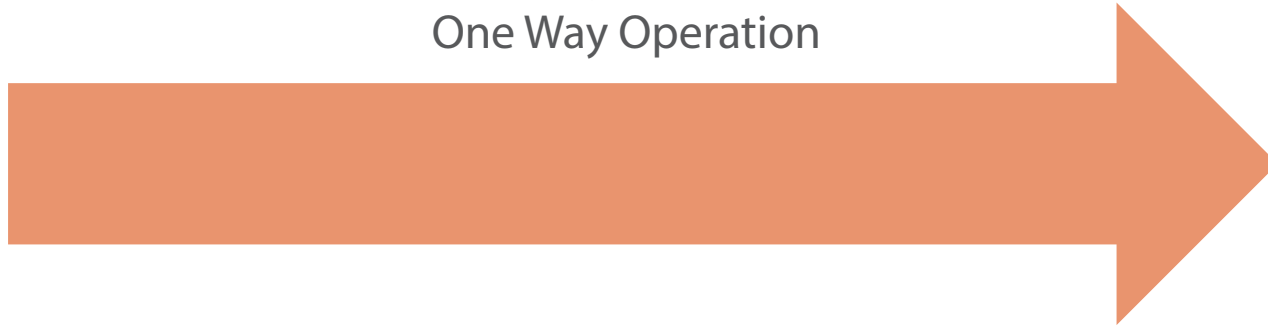
What Is Hashing?



What Is Hashing?

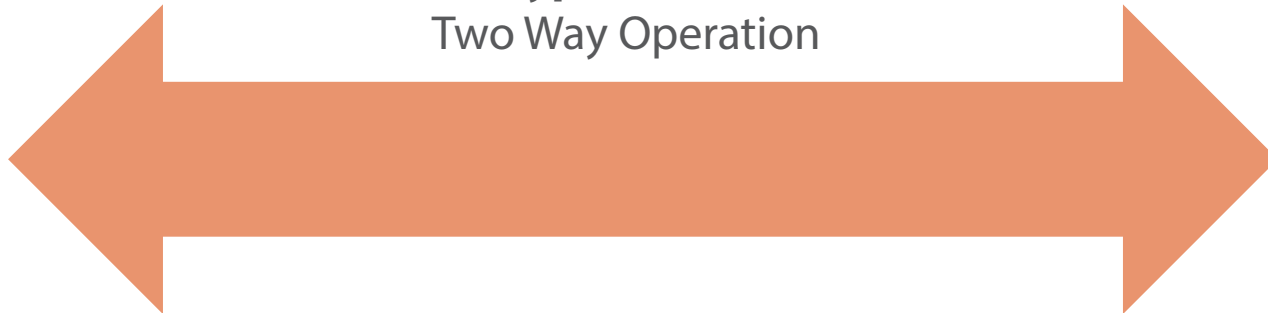
Hashing

One Way Operation

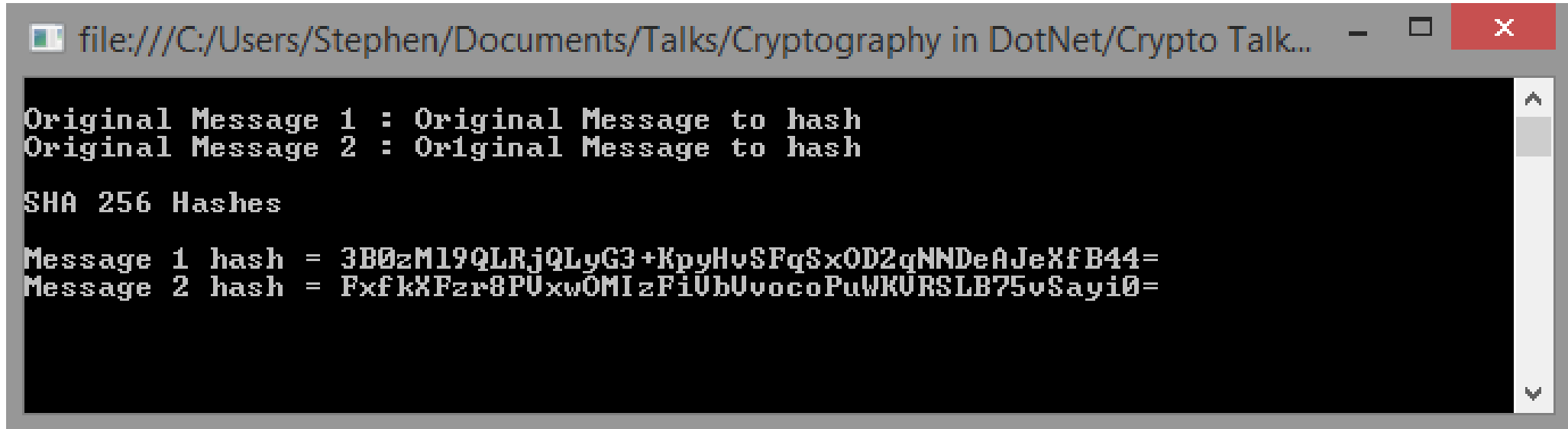


Encryption

Two Way Operation



What Is Hashing?



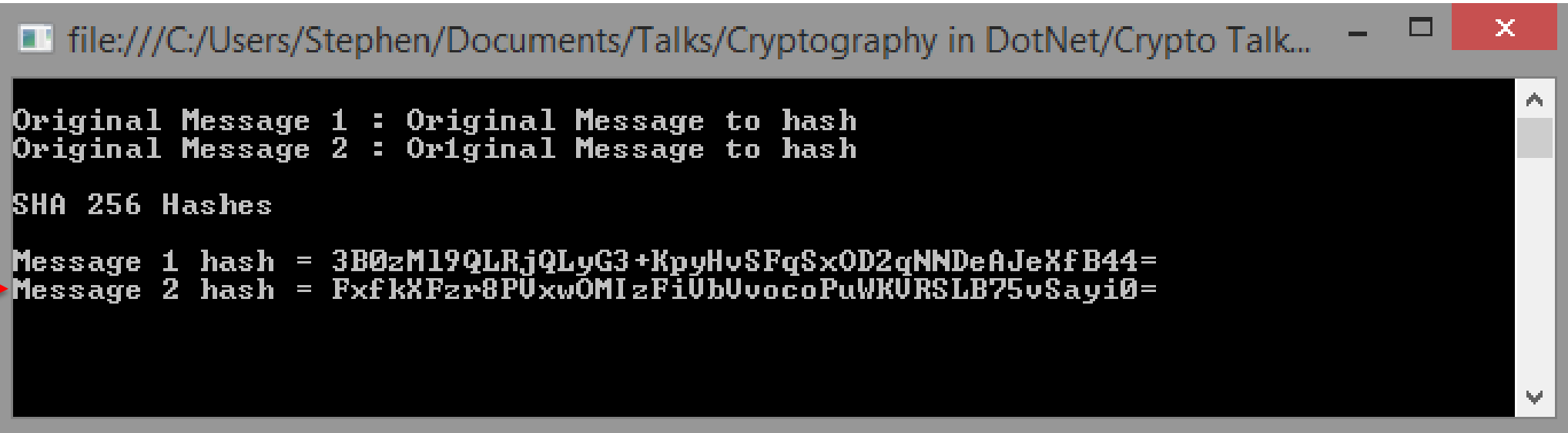
A screenshot of a Windows file explorer window. The title bar shows the file path: `file:///C:/Users/Stephen/Documents/Talks/Cryptography in DotNet/Crypto Talk...`. The window contains a text file with the following content:

```
Original Message 1 : Original Message to hash
Original Message 2 : Original Message to hash

SHA 256 Hashes

Message 1 hash = 3B0zM19QLRjQLyG3+KpυHυSFqSxOD2qNNDeAJeXfB44=
Message 2 hash = FxfkXFzr8PUxwOMIzFiUhUvocoPuWKURSLB75υSayi0=
```

What Is Hashing?



A screenshot of a Windows file explorer window. The title bar shows the file path: `file:///C:/Users/Stephen/Documents/Talks/Cryptography in DotNet/Crypto Talk...`. The window contains a text file with the following content:

```
Original Message 1 : Original Message to hash
Original Message 2 : Original Message to hash

SHA 256 Hashes

Message 1 hash = 3B0zM19QLRjQLyG3+KpυHυSFqSxOD2qNNDeAJeXfB44=
Message 2 hash = FxfkXFzr8PUxwOMIzFiUbUvocoPuWKURSLB75υSayi0=
```

A red arrow points to the first hash value: `3B0zM19QLRjQLyG3+KpυHυSFqSxOD2qNNDeAJeXfB44=`.

What Is Hashing?

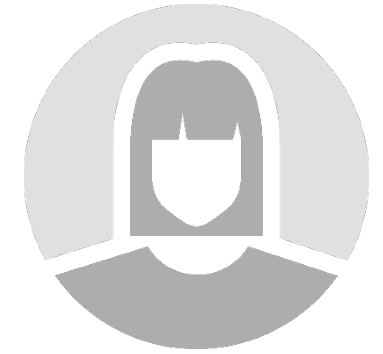
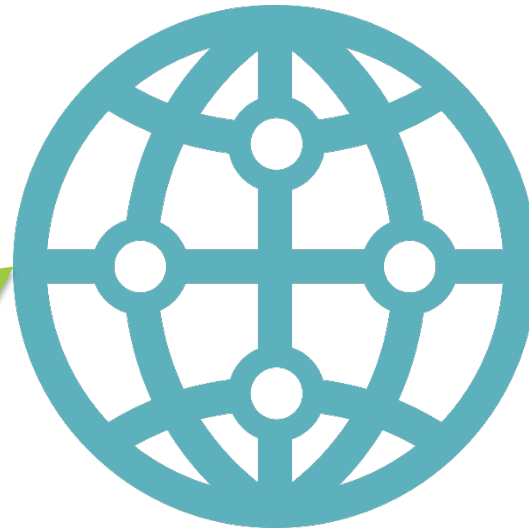


Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=



Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=

What Is Hashing?

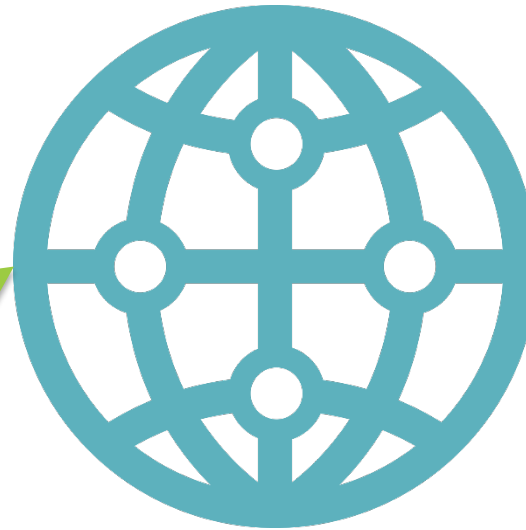


Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=



Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=

What Is Hashing?

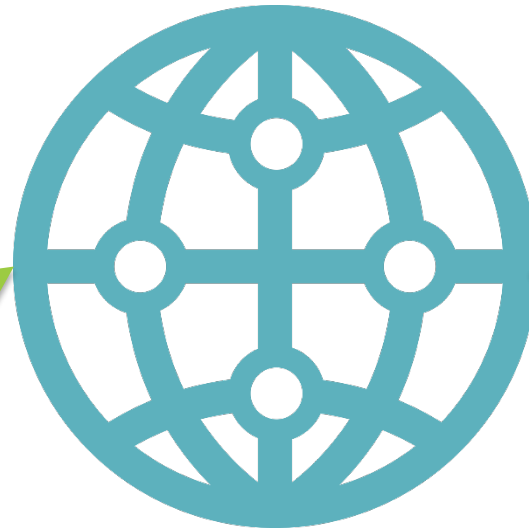


Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=



Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=

What Is Hashing?

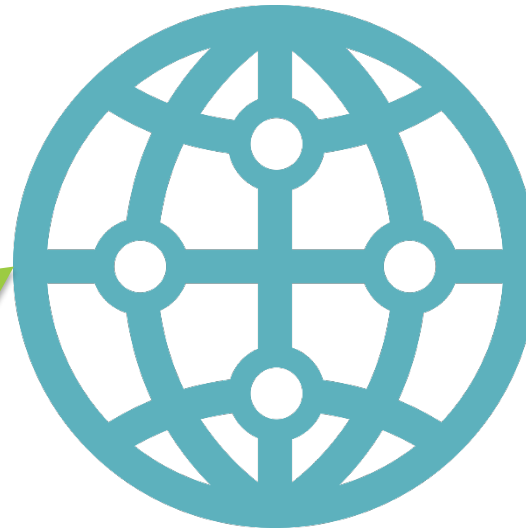


Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=



Message

Meet me at the coffee shop to exchange the contracts.

Hash

3897yrwnvymt98w3r5c982m=

567iuj45tf24r23er32f243f234r=

MD5

- Designed by Ron Rivest in 1991 to replace MD4
- Produces a 128 bit (16 byte) hash value
- Commonly used to verify file integrity
- First collision resistance flaw found in 1996
- Recommendation was to move over to the Secure Hash Family
- Further collision resistance problems found in 2004
- Still needed when integrating with legacy systems

Secure Hash (SHA) Family

SHA-1

SHA-2

SHA-3

Code Demo

Hashing with MD5 and the SHA Family

Hashed Message Authentication Codes

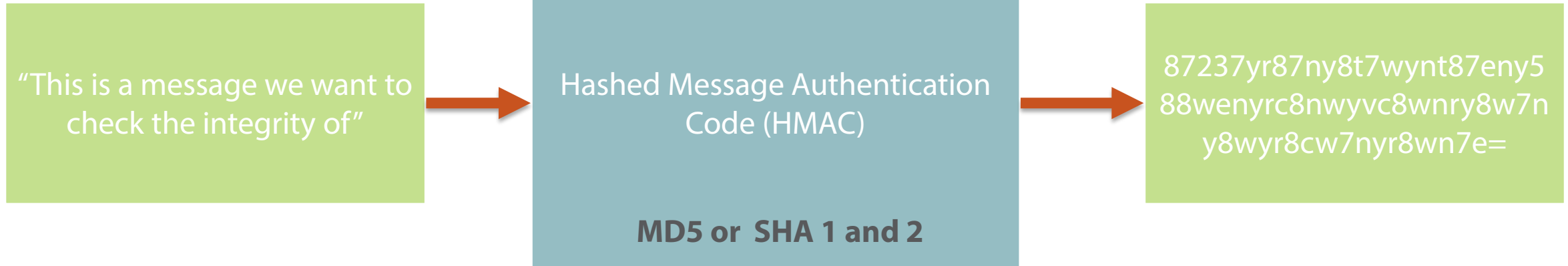


"This is a message we want to check the integrity of"

Hashed Message Authentication Code (HMAC)

87237yr87ny8t7wynt87eny5
88wenyrc8nwyvc8wnry8w7n
y8wyr8cw7nyr8wn7e=

Hashed Message Authentication Codes



Code Demo

Hashed Message Authentication Codes

Module Summary



- What is Hashing?
- MD5
- Secure Hash (SHA) Family
- Hashed Message Authentication Codes (HMAC)