Structure

SHA256

An implementation of Secure Hashing Algorithm 2 (SHA-2) hashing with a 256-bit digest.

iOS 13.0+ | iPadOS 13.0+ | Mac Catalyst 13.0+ | macOS 10.15+ | tvOS 13.0+ | visionOS 1.0+ | watchOS 6.0+

```
struct SHA256
```

Overview

The SHA256 hash implements the HashFunction protocol for the specific case of SHA-2 hashing with a 256-bit digest (SHA256Digest). Larger digests take more space but are more secure.

You can compute the digest by calling the static `hash(data:)` method once. Alternatively, if the data that you want to hash is too large to fit in memory, you can compute the digest iteratively by creating a new hash instance, calling the `update(data:)` method repeatedly with blocks of data, and then calling the `finalize()` method to get the result.

Topics

Specifying the output type

`typealias` **Digest**

The digest type for a SHA256 hash function.

`struct` **SHA256Digest**

The output of a Secure Hashing Algorithm 2 (SHA-2) hash with a 256-bit digest.

Computing a hash iteratively

`init()`

Creates a SHA256 hash function.

`func update(bufferPointer: UnsafeRawBufferPointer)`

Incrementally updates the hash function with the contents of the buffer.

`func finalize() -> SHA256.Digest`

Finalizes the hash function and returns the computed digest.

Inspecting hash information

`static let byteCount: Int`

The number of bytes in a SHA256 digest.

`static let blockByteCount: Int`

The number of bytes that represents the hash function's internal state.

Relationships

Conforms To

`Copyable`
`HashFunction`
`Sendable`
`SendableMetatype`

See Also

Cryptographically secure hashes

`protocol HashFunction`

A type that performs cryptographically secure hashing.

`struct` SHA512

An implementation of Secure Hashing Algorithm 2 (SHA-2) hashing with a 512-bit digest.

`struct` SHA384

An implementation of Secure Hashing Algorithm 2 (SHA-2) hashing with a 384-bit digest.