

[Apple CryptoKit](#) / ChaChaPoly

Enumeration

ChaChaPoly

An implementation of the ChaCha20-Poly1305 cipher.

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

`enum` ChaChaPoly

Topics

Storing the output

`struct` SealedBox

A secure container for your data that you access using a cipher.

Getting a nonce

`struct` Nonce

A value used once during a cryptographic operation and then discarded.

Securing the plaintext message

```
static func seal<Plaintext>(Plaintext, using: SymmetricKey, nonce: ChaChaPoly.Nonce?) throws -> ChaChaPoly.SealedBox
```

Secures the given plaintext message with encryption and an authentication tag.

```
static func seal<Plaintext, AuthenticatedData>(Plaintext, using:
SymmetricKey, nonce: ChaChaPoly.Nonce?, authenticating: Authenticated
Data) throws -> ChaChaPoly.SealedBox
```

Secures the given plaintext message with encryption and an authentication tag that covers both the encrypted data and additional data.

Decrypting and verifying the message

```
static func open(ChaChaPoly.SealedBox, using: SymmetricKey) throws ->
Data
```

Decrypts the message and verifies its authenticity.

```
static func open<AuthenticatedData>(ChaChaPoly.SealedBox, using:
SymmetricKey, authenticating: AuthenticatedData) throws -> Data
```

Decrypts the message and verifies the authenticity of both the encrypted message and additional data.

Relationships

Conforms To

Sendable, SendableMetatype

See Also

Ciphers

enum AES

A container for Advanced Encryption Standard (AES) ciphers.