aes

package standard library

Version: go1.20.1 Latest | Published: Feb 14, 2023 | License: BSD-3-Clause | Imports: 9 |
Imported by: 21,908

Details ✓ Valid go.mod file ? ✓ Redistributable license ? ✓ Tagged version ?
✓ Stable version ?
Learn more

Repository cs.opensource.google/go/go

Links Report a Vulnerability

Documentation

Documentation

Rendered for linux/amd64

Overview

Package aes implements AES encryption (formerly Rijndael), as defined in U.S. Federal Information Processing Standards Publication 197.

The AES operations in this package are not implemented using constant-time algorithms. An exception is when running on systems with enabled hardware support for AES that makes these operations constant-time. Examples include amd64 systems using AES-NI extensions and s390x systems using Message-Security-Assist extensions. On such systems, when the result of NewCipher is passed to cipher.NewGCM, the GHASH operation used by GCM is also constant-time.

Index

Constants

View Source

```
const BlockSize = 16
```

The AES block size in bytes.

Variables

This section is empty.

Functions

func NewCipher

```
func NewCipher(key []byte) (cipher.Block, error)
```

NewCipher creates and returns a new cipher.Block. The key argument should be the AES key, either 16, 24, or 32 bytes to select AES-128, AES-192, or AES-256.

Types

type KeySizeError

```
type KeySizeError int
```

func (KeySizeError) Error

```
func (k KeySizeError) Error() string
```

Source Files

View all

aes_gcm.go
block.go
cipher.go
cipher_asm.go
const.go
modes.go

GitHub

Slack

r/golang

Meetup

Golang Weekly

Copyright

Terms of Service

Privacy Policy

Report an Issue