

Discover Packages > Standard library > crypto > subtle 

subtle


package

standard library

Version: [go1.20.1](#) **Latest** | Published: Feb 14, 2023 | License: [BSD-3-Clause](#) | Imports: 0 |

Imported by: [13,551](#)

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 `subtle` implements functions that are often useful in cryptographic code but require careful thought to use correctly.

Index

```
func ConstantTimeByteEq(x, y uint8) int
func ConstantTimeCompare(x, y []byte) int
func ConstantTimeCopy(v int, x, y []byte)
func ConstantTimeEq(x, y int32) int
func ConstantTimeLessOrEq(x, y int) int
func ConstantTimeSelect(v, x, y int) int
func XORBytes(dst, x, y []byte) int
```

Constants

This section is empty.

Variables

This section is empty.

Functions

func [ConstantTimeByteEq](#)

```
func ConstantTimeByteEq(x, y uint8) int
```

ConstantTimeByteEq returns 1 if $x == y$ and 0 otherwise.

func ConstantTimeCompare

```
func ConstantTimeCompare(x, y []byte) int
```

ConstantTimeCompare returns 1 if the two slices, x and y , have equal contents and 0 otherwise. The time taken is a function of the length of the slices and is independent of the contents. If the lengths of x and y do not match it returns 0 immediately.

func ConstantTimeCopy

```
func ConstantTimeCopy(v int, x, y []byte)
```

ConstantTimeCopy copies the contents of y into x (a slice of equal length) if $v == 1$. If $v == 0$, x is left unchanged. Its behavior is undefined if v takes any other value.

func ConstantTimeEq

```
func ConstantTimeEq(x, y int32) int
```

ConstantTimeEq returns 1 if $x == y$ and 0 otherwise.

func ConstantTimeLessOrEq

added in go1.2

```
func ConstantTimeLessOrEq(x, y int) int
```

ConstantTimeLessOrEq returns 1 if $x \leq y$ and 0 otherwise. Its behavior is undefined if x or y are negative or $> 2^{31} - 1$.

func ConstantTimeSelect

```
func ConstantTimeSelect(v, x, y int) int
```

ConstantTimeSelect returns x if $v == 1$ and y if $v == 0$. Its behavior is undefined if v takes any other value.

func XORBytes

added in go1.20

```
func XORBytes(dst, x, y []byte) int
```

XORBytes sets $dst[i] = x[i] \oplus y[i]$ for all $i < n = \min(\text{len}(x), \text{len}(y))$, returning n , the number of bytes written to dst . If dst does not have length at least n , XORBytes panics without writing anything to dst .

Types

This section is empty.



[constant_time.go](#)

[xor.go](#)

[xor_amd64.go](#)

Why Go

[Use Cases](#)

[Case Studies](#)

Get Started

[Playground](#)

[Tour](#)

[Stack Overflow](#)

[Help](#)

Packages

[Standard Library](#)

[About Go Packages](#)

About

[Download](#)

[Blog](#)

[Issue Tracker](#)

[Release Notes](#)

[Brand Guidelines](#)

[Code of Conduct](#)

Connect

[Twitter](#)

[GitHub](#)

[Slack](#)

[r/golang](#)

[Meetup](#)

[Golang Weekly](#)

[Copyright](#)

[Terms of Service](#)

[Privacy Policy](#)

[Report an Issue](#)

