Package 'cryptorng'

April 28, 2024

Type Package

Title Access System Cryptographic Pseudorandom Number Generators

Version 0.1.2

Maintainer Mike Cheng <mikefc@coolbutuseless.com>

Description Generate random bytes from the Cryptographically Secure Pseudorandom Number Generator (CSPRNG) provided by the underlying operating system. These system CSPRNGs are seeded internally by the OS with entropy it gathers and use random number generation algorithms which are considered cryptographically secure. The following system functions are used: arc4random_buf() on macOS and BSD; BCryptgenRandom() on Windows; Sys_getrandom() on Linux.

License MIT + file LICENSE

Encoding UTF-8

RoxygenNote 7.3.1

Suggests testthat (>= 3.0.0)

Config/testthat/edition 3

URL https://github.com/coolbutuseless/cryptorng

BugReports https://github.com/coolbutuseless/cryptorng/issues

NeedsCompilation yes

Author Mike Cheng [aut, cre, cph]

Repository CRAN

Date/Publication 2024-04-28 10:50:03 UTC

R topics documented:

`rcrypto` *Generate random bytes from the platform-specific cryptographically secure pseudorandom number generator*

Description

Generate random bytes from the platform-specific cryptographically secure pseudorandom number generator

Usage

```
rcrypto(n, type = "raw")
```

Arguments

`n`	Number of random bytes to generate. Note: if the entropy pool is exhausted on your system it may not be able to provide the requested number of bytes - in this case an error is thrown.
`type`	Type of returned values - 'raw' or 'string'. Default: 'raw'.

Value

A raw vector or a hexadecimal string

Platform notes

The method used for generating random values varies depending on the operating system (OS):

- For macOS and BSDs: `arc4random_buf()`
- For linux: `syscall(SYS_getrandom())`
- For win32: `BCryptGenRandom()`

All these random number generators are internally seeded by the OS using entropy gathered from multiple sources and are considered cryptographically secure.

Examples

```
rcrypto(16, type = 'string')
rcrypto(16, type = 'raw')
```

Index