Package ‘scrypt’
April 19, 2022

Type Package
Title Key Derivation Functions for R Based on Scrypt
Version 0.1.4
Copyright RStudio, Inc.; Colin Percival
Maintainer Bob Jansen <bobjansen@gmail.com>
Description Functions for working with the scrypt key derivation functions
originally described by Colin Percival
<https://www.tarsnap.com/scrypt/scrypt.pdf> and in Percival and Josefsson
(2016) <doi:10.17487/RFC7914>. Scrypt is a password-based key derivation
function created by Colin Percival. The algorithm was specifically designed
to make it costly to perform large-scale custom hardware attacks by
requiring large amounts of memory.
License FreeBSD
Depends R (>= 3.0.0)
URL https://github.com/rstudio/rscrypt
Imports Rcpp (>= 0.10.6)
LinkingTo Rcpp
NeedsCompilation yes
Author Bob Jansen [ctb, cre],
Andy Kipp [aut],
Colin Percival [aut, cph],
RStudio [cph]
Repository CRAN
Date/Publication 2022-04-19 11:30:02 UTC

R topics documented:

scrypt-package ............................................................ 2
hashPassword .............................................................. 2
verifyPassword ............................................................. 3

Index 5
scrypt-package scrypt key derivation functions for R

Description

scrypt is an R package for working with scrypt. Scrypt is a password-based key derivation function created by Colin Percival. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory.

Details

Package: scrypt
Type: Package
Version: 0.1
Date: 2014-01-07
License: GPLv3

The scrypt package can be used for hashing and verifying passwords, or encrypting and decrypting data. Additionally, the scrypt function can be used directly.

Author(s)

RStudio, Inc.; Colin Percival Maintainer: Andy Kipp <andy@rstudio.com>

References

scrypt

See Also

hashPassword, verifyPassword and scrypt

hashPassword

Hash a password

Description

Hash a password

Usage

hashPassword(passwd, maxmem = 0.1, maxtime = 1)
verifyPassword

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwd</td>
<td>password to hash</td>
</tr>
<tr>
<td>maxmem</td>
<td>max memory percent (default 0.1)</td>
</tr>
<tr>
<td>maxtime</td>
<td>max cpu time (default 1.0)</td>
</tr>
</tbody>
</table>

Value

base64 encoded hash

See Also

verifyPassword

Examples

# Hash password using default parameters
hashPassword('passw0rd')

# Hash password with custom parameters
hashPassword('passw0rd', maxmem=0.25, maxtime=1.0)

verifyPassword

Verify a hashed password

Description

Verify a hashed password

Usage

verifyPassword(hash, passwd)

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash</td>
<td>base64 hash to verify</td>
</tr>
<tr>
<td>passwd</td>
<td>password to verify</td>
</tr>
</tbody>
</table>

Value

TRUE if password matches hash, otherwise FALSE

See Also

hashPassword
Examples

# Hash password using default parameters
hashed <- hashPassword("password")

# verify invalid password
verifyPassword(hashed, "bad password");

# verify correct password
verifyPassword(hashed, "password")
Index

* package
  scrypt-package, 2

hashPassword, 2, 2, 3

rscrypt (scrypt-package), 2

scrypt, 2
scrypt (scrypt-package), 2
scrypt-package, 2

verifyPassword, 2, 3, 3