Package 'rcrypt'

August 29, 2016

Title Symmetric File Encryption Using GPG

Version 0.1.1

Description Provides easy symmetric file encryption using GPG with cryptographically strong defaults. Only symmetric encryption is supported. GPG is pre-installed with most Linux distributions. Windows users will need to install 'Gpg4win' (http://www.gpg4win.org/). OS X users will need to install 'GPGTools' (https://gpgtools.org/).

URL http://brettklamer.com/work/rcrypt/

Depends R (>= 3.0.0)

SystemRequirements GnuPG (https://gnupg.org/)

License MIT + file LICENSE

LazyData true

Suggests testthat

NeedsCompilation no

Author Brett Klamer [aut, cre]

Maintainer Brett Klamer <rcrypt@brettklamer.com>

Repository CRAN

Date/Publication 2015-09-20 08:01:09

R topics documented:

decrypt *Decrypt a File Using GPG*

Description

Decrypt a symmetrically encrypted file using GPG.

Usage

```
decrypt(input, output = NULL, passphrase = NULL, verbosity = 1)
```

Arguments

input	A character string of the file name you wish to decrypt.
output	A character string of the file name that will be created. The default is to create a file with the same name (stripped of the .gpg or .asc file extension) in the same folder.
passphrase	A character string of the passphrase used to decrypt the encrypted file. WARNING: use this to bypass the more secure option of GPG's passphrase popup box. WARNING: the passphrase may be saved in the script as cleartext, saved in the terminal history in cleartext, and/or available in the list of processes in cleartext. The default value is NULL (Insert the passphrase using GPG's secure pop-up box).
verbosity	An integer 0, 1, 2, or 3. Control GPG's terminal message information in increasing level of detail. A value of 0 passes the '--quiet' flag for a minimum amount of information. A value of 1 does not pass any flags. A value of 2 passes the '--verbose' flag. A value of 3 passes the '--verbose --verbose' flag for the most information. The default value is 1.

Value

A decrypted file.

Examples

```
## Not run:
decrypt("path/to/your/file.csv.gpg")
decrypt("path/to/your/file.csv.gpg", output = "path/to/your/file.csv")
# WARNING: only use the passphrase argument if you understand why it's
# not secure.
decrypt("path/to/your/file.csv.gpg", passphrase = "your-passphrase")

## End(Not run)
```

encrypt *Encrypt a File Using GPG.*

Description

Symmetric file encryption using GPG. The encrypt function defaults to the strongest cryptographic flags available for GPG.

Usage

```
encrypt(input, output = NULL, passphrase = NULL, compress = "ZLIB",
  cipher = "AES256", armor = FALSE, mdc = TRUE, s2k.mode = 3,
  s2k.digest = "SHA512", s2k.count = 65011712, verbosity = 1)
```

Arguments

input	A character string of the file name you wish to encrypt.
output	A character string of the file name that will be created. The default is to create a file with the same name (with an additional .gpg or .asc file extension) in the same folder.
passphrase	A character string of the passphrase used to decrypt the encrypted file. WARNING: use this to bypass the more secure option of GPG's passphrase popup box. WARNING: the passphrase may be saved in the script as cleartext, saved in the terminal history in cleartext, and/or available in the list of processes in cleartext. The default value is NULL (Insert the passphrase using GPG's secure pop-up box).
compress	A character string of the methods of compression. Possible values are "Uncompressed", "ZIP", "ZLIB", and "BZIP2". Values depend on your GPG installation. The default value is "ZLIB".
cipher	A character string of the encryption algorithm. Possible values are "AES256", "Camellia256", "TWOFISH", "AES128", etc. Values depend on your GPG installation. The default value is "AES256".
armor	TRUE or FALSE: flag to produce an encrypted ASCII text output file. The default value is FALSE.
mdc	TRUE or FALSE: flag to force the use of modification detection code. It is always used with newer encryption algorithms and recommended to always keep TRUE. The default value is TRUE.
s2k.mode	An integer 0, 1, or 3. Sets how passphrases are mangled. A value of 0 just uses a plain passphrase (never use). A value of 1 will add a salt to the passphrase. A value of 3 will salt and iterate the passphrase. It is highly recommended to always use 3. The default value is 3.
s2k.digest	A character string of the digest algorithm used to mangle passphrases. Possible values are "SHA512", "SHA384", "SHA256", etc. The default value is "SHA512".
s2k.count	An integer between 1024 and 65011712. Specifies how many times the passphrase mangling is repeated. The default value is 65011712.

`verbosity` An integer `0`, `1`, `2`, or `3`. Control GPG's terminal message information in increasing level of detail. A value of `0` passes the `'--quiet'` flag for a minimum amount of information. A value of `1` does not pass any flags. A value of `2` passes the `'--verbose'` flag. A value of `3` passes the `'--verbose --verbose'` flag for the most information. The default value is `1`.

Value

An encrypted file.

Examples

```
## Not run:
encrypt("path/to/your/file.csv")
encrypt("path/to/your/file.csv", output = "path/to/your/file.csv.gpg")
# WARNING: only use the passphrase argument if you understand why it's
# not secure.
encrypt("path/to/your/file.csv", passphrase = "your-passphrase")

## End(Not run)
```

Index