Package ‘cryptography’

July 8, 2023

Title Encrypts and Decrypts Text Ciphers
Version 1.0.0
Description Playfair, Four-Square, Scytale, Columnar Transposition and Autokey methods. Further explanation on methods of classical cryptography can be found at Wikipedia; (<https://en.wikipedia.org/wiki/Classical_cipher>).
License MIT + file LICENSE
Encoding UTF-8
RoxygenNote 7.2.3
Suggests knitr, rmarkdown, testthat (>= 3.0.0)
Config/testthat/edition 3
URL https://github.com/PiarasFahey/cryptography
BugReports https://github.com/PiarasFahey/cryptography/issues
Imports DescTools
VignetteBuilder knitr
NeedsCompilation no
Author Piaras Fahey [aut, cre, cph]
Maintainer Piaras Fahey <faheypi@tcd.ie>
Repository CRAN
Date/Publication 2023-07-08 09:40:02 UTC

R topics documented:

autokey ................................................................. 2
columnar_transposition ........................................... 2
four_square ............................................................ 3
playfair ................................................................. 4
scytale ................................................................. 4

Index 6
**Autokey Cipher**

**Description**
This can be used to encrypt or decrypt an Autokey cipher. The Autokey Cipher is derived from the Vigenere Cipher, in which the key and plaintext are bound to generate a new encryption key for the Vigenere method. This Vigenere method uses only letters and numbers, as such any other characters used as inputs are not used in the cipher.

**Usage**
```
autokey(message, key, encrypt = TRUE)
```

**Arguments**
- **message**: A character vector of plaintext to be encrypted or ciphertext to be decrypted
- **key**: A character vector to be used as the encryption key
- **encrypt**: (Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.

**Value**
A character vector of either plaintext that has been encrypted or ciphertext that has been decrypted.

**Examples**
```
autokey("VerySecretMessage", "Hack", encrypt = TRUE)
autokey("c4JYn8JfwNoLMbmAM", "Hack", encrypt = FALSE)
autokey("Very $%^&SecretMes(*sag£$e", "Hack", encrypt = TRUE)
```

---

**Columnar Transposition Cipher**

**Description**
This can be used to encrypt or decrypt a Columnar Transposition cipher. This method is a development of the Scytale cipher that rearranges the encryption matrix used in the Scytale method by the alphabetical ordering of the encryption key.

**Usage**
```
columnar_transposition(message, key, encrypt = TRUE)
```
four_square

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>A character vector</td>
</tr>
<tr>
<td>key</td>
<td>A character vector composed only of a-zA-Z letters used as the encryption key (Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.</td>
</tr>
<tr>
<td>encrypt</td>
<td>(Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.</td>
</tr>
</tbody>
</table>

Value

A character vector of either plaintext that has been encrypted or ciphertext that has been decrypted using the columnar transposition cryptographic method.

Examples

columnar_transposition("Hidden message", "hack", encrypt = TRUE)
columnar_transposition("insed sHeegdma", "hack", encrypt = FALSE)

four_square

Four-Square Cipher

Description

This can be used to encrypt or decrypt a Four-Square cipher. The Four-Square cipher is a polygraphic substitution cipher that maps digrams of text to two encryption matrices through their position in a square alphabet matrix.

Usage

four_square(message, key1, key2, encrypt = TRUE)

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>a character vector used as the plaintext to be encrypted or the ciphertext to be decrypted</td>
</tr>
<tr>
<td>key1</td>
<td>a character vector used as the encryption key for the first encryption matrix</td>
</tr>
<tr>
<td>key2</td>
<td>a character vector used as the encryption key for the second encryption matrix (Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.</td>
</tr>
<tr>
<td>encrypt</td>
<td>(Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.</td>
</tr>
</tbody>
</table>

Value

A character vector of either plaintext that has been encrypted or ciphertext that has been decrypted.

Examples

four_square("THEPRISONERSHAVEESCAPED", "HACK", "SAFE", encrypt = TRUE)
four_square("SHBOTDMPFSQDFZSCUHFPBCY", "HACK", "SAFE", encrypt = FALSE)
**playfair**

*Playfair Cipher*

**Description**

This can be used to encrypt or decrypt a Playfair cipher. A Playfair cipher is a polygraphic substitution cipher that maps digrams of text to other elements of an encryption matrix which is generated by a keyword.

**Usage**

`playfair(message, key, encrypt = TRUE)`

**Arguments**

- `message`: a character vector to be encrypted or decrypted
- `key`: a character vector to be used as the encryption key
- `encrypt`: (Default: `TRUE`) `TRUE` will encrypt the message, while `FALSE` will decrypt the message.

**Value**

A character vector of either plaintext that has been encrypted or ciphertext that has been decrypted.

**Examples**

`playfair("SUPERSECRETMESSAGE", "safety", encrypt = TRUE)`

`playfair("YSQFNTFDQTGRTAAFDT", "safety", encrypt = FALSE)`

`playfair("%`.Att&a@9CK__He88re", "safety", encrypt = TRUE)`

`playfair("FSSFKPL5QT", "safety", encrypt = FALSE)`

---

**scytale**

*Scytale cipher*

**Description**

This can be used to encrypt and decrypt a Scytale cipher. A Scytale cipher is an ancient form of cryptography that wraps a message (typically written on a long thing piece of paper) around a device to create a matrix with a fixed number of columns that transposes the text.

**Usage**

`scytale(message, col, encrypt = TRUE)`
Arguments

message    A character vector

col    A positive integer, this determines the number of columns in the encryption matrix. 1 column will have no effect

encrypt    (Default: TRUE) TRUE will encrypt the message, while FALSE will decrypt the message.

Value

A character vector of either plaintext that has been encrypted or ciphertext that has been decrypted.

Examples

scytale("very super secret message!", col = 4, encrypt = TRUE)
scytale("v eetseesrc slru rmaypseeg", col = 4, encrypt = FALSE)
Index

autokey, 2
columnar_transposition, 2
four_square, 3
playfair, 4
scytale, 4