NAME

md5 – calculate a message-digest fingerprint (checksum) for a file

SYNOPSIS

md5 [-t | -x | -sstring | filename(s)]

DESCRIPTION

md5 takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as *RSA.*

OPTIONS

The following four options may be used in any combination, except that **filename(s)** must be the last objects on the command line.

-sstring prints a checksum of the given "string".

-t runs a built-in time trial.

-x runs a built-in test script.

filename(s) prints a checksum(s) for each of the files.

SEE ALSO

sum(1)

RFC 1321 describes in detail the MD2, MD4, and MD5 message-digest algorithms.

ACKNOWLEDGEMENTS

This program is placed in the public domain for free general use by RSA Data Security.