NAME

MD5, **MD5Init**, **MD5Transform** - message digest routines

SYNOPSIS

#include <sys/types.h>
#include <sys/md5.h>

void
MD5Init(*MD5_CTX *buf*);

void
MD5Transform(*uint32_t buf[4], const unsigned char block[64]*);

DESCRIPTION

The **MD5** module implements the RSA Data Security, Inc. MD5 Message-Digest Algorithm (MD5). It produces 128-bit MD5 Digest of data.

MD5Init must be called just before **MD5Transform**() will be used to produce a digest. The *buf* argument is the storage for the digest being produced on subsequent calls to the **MD5Transform**() routine.

MD5Transform is the core of the MD5 algorithm, this alters an existing MD5 hash kept in *buf* to reflect the addition of 64 characters of new data passed in *block* argument.

COPYRIGHTS

The code for MD5 transform was taken from Colin Plumb's implementation, which has been placed in the public domain. The MD5 cryptographic checksum was devised by Ronald Rivest, and is documented in RFC 1321, "The MD5 Message Digest Algorithm".