

MD4 (RFC-1320) message digest.

Modified from MD5 code by Andrey Panin <pazke@donpac.ru>

Written by Solar Designer <solar@openwall.com> in 2001, and placed in the public domain. There's absolutely no warranty.

See `src/3rdparty/md4/md4.cpp` and `src/3rdparty/md4/md4.h` for more information about the terms and conditions under which the code is supplied.

=== (copied from md4.cpp) ===

/*

* MD4 (RFC-1320) message digest.

* Modified from MD5 code by Andrey Panin <pazke@donpac.ru>

*

* Written by Solar Designer <solar@openwall.com> in 2001, and placed in

* the public domain. There's absolutely no warranty.

*

* This differs from Colin Plumb's older public domain implementation in

* that no 32-bit integer data type is required, there's no compile-time

* endianness configuration, and the function prototypes match OpenSSL's.

* The primary goals are portability and ease of use.

*

* This implementation is meant to be fast, but not as fast as possible.

* Some known optimizations are not included to reduce source code size

* and avoid compile-time configuration.

*/

===