Compilation Copyright (c) 1995-2019 by Wei Dai. All rights reserved.

This copyright applies only to this software distribution package

as a compilation, and does not imply a copyright on any particular

file in the package.

All individual files in this compilation are placed in the public domain by

Wei Dai and other contributors.

I would like to thank the following authors for placing their works into

the public domain:

Joan Daemen - 3way.cpp

Leonard Janke - cast.cpp, seal.cpp

Steve Reid - cast.cpp

Phil Karn - des.cpp

Andrew M. Kuchling - md2.cpp, md4.cpp

Colin Plumb - md5.cpp

Seal Woods - rc6.cpp

Chris Morgan - rijndael.cpp

Paulo Baretto - rijndael.cpp, skipjack.cpp, square.cpp

Richard De Moliner - safer.cpp

Matthew Skala - twofish.cpp

Kevin Springle - camellia.cpp, shacal2.cpp, ttmac.cpp, whrlpool.cpp, ripemd.cpp

Ronny Van Keer - sha3.cpp

Aumasson, Neves, Wilcox-O'Hearn and Winnerlein - blake2.cpp, blake2b\_simd.cpp, blake2s\_simd.cpp

Aaram Yun - aria.cpp, aria\_simd.cpp

Han Lulu, Markku-Juhani O. Saarinen - sm4.cpp sm4\_simd.cpp

Daniel J. Bernstein, Jack Lloyd - chacha.cpp, chacha\_simd.cpp, chacha\_avx.cpp

Andrew Moon - ed25519, x25519, donna\_32.cpp, donna\_64.cpp, donna\_sse.cpp

The Crypto++ Library uses portions of Andy Polyakov's CRYPTOGAMS on Linux

for 32-bit ARM with files aes\_armv4.S, sha1\_armv4.S and sha256\_armv4.S.

CRYPTOGAMS is dual licensed with a permissive BSD-style license. The

CRYPTOGAMS license is reproduced below. You can disable Cryptogams code by

undefining the relevant macros in config\_asm.h.

The Crypto++ Library uses portions of Jack Lloyd's Botan for ChaCha SSE2 and

AVX. Botan placed the code in public domain for Crypto++ to use.

The Crypto++ Library (as a compilation) is currently licensed under the Boost

Software License 1.0 (http://www.boost.org/users/license.html).

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization

obtaining a copy of the software and accompanying documentation covered by

this license (the "Software") to use, reproduce, display, distribute,

execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to

do so, all subject to the following:

The copyright notices in the Software and this entire statement, including

the above license grant, this restriction and the following disclaimer,

must be included in all copies of the Software, in whole or in part, and

all derivative works of the Software, unless such copies or derivative

works are solely in the form of machine-executable object code generated by

a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT

SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE

FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER

DEALINGS IN THE SOFTWARE.

CRYPTOGAMS License

Copyright (c) 2006-2017, CRYPTOGAMS by <appro@openssl.org>

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions

are met:

\* Redistributions of source code must retain copyright notices,

this list of conditions and the following disclaimer.

\* Redistributions in binary form must reproduce the above

copyright notice, this list of conditions and the following

disclaimer in the documentation and/or other materials

provided with the distribution.

\* Neither the name of the CRYPTOGAMS nor the names of its copyright

holder and contributors may be used to endorse or promote products

derived from this software without specific prior written permission.