Authors of GNU Nettle

The oldest code in Nettle was copied into precursors of the Nettle

library from other public domain or LGPLv2 sources.

Steve Reid Original CAST128 implementation

Dana L. How Original DES implementation,

Colin Plumb Original MD5 implementation

Peter Gutmann Original SHA1 implementation

Andrew Kuchling Original MD2 implementation

Free Software Foundation

Holds copyrights on code ported from

libgcrypt, written by Werner Koch and others.

J.H.M. Dassen Original port of blowfish to GNU lsh, later

split off into Nettle. (This blowfish

implementation was replaced later).

Twofish tests.

Ruud de Rooij Twofish implementation for GNU lsh, later split off into Nettle.

Rafael Sevilla AES C and x86 implementation, original port of

Serpent, for GNU lsh, later split off into Nettle.

Authors of Nettle (in roughly chronological order of initial contribution)

Niels Möller Main author.

Dan Egnor Base64 conversion.

Andreas Sigfridsson Port of MD2, from Andrew Kuchling's python

cryptography toolkit.

Marcus Comstedt Implemented MD4.

D. J. Bernstein Salsa20 public domain reference implementation.

Simon Josefsson Port of Arctwo, from GnuTLS and libgcrypt. New

ports of LGPL Serpent and Blowfish code, from

libgcrypt. Port of Salsa20, based on djb's

reference. Implementation of PBKDF2 (RFC

2898).

Henrik Grubbström AES assembly for Sparc64.

Magnus Holmgren Conversion of DSA keys from DER format to SEXP

format.

Daniel Kahn Gillmor Added the lists for nettle\_get\_ciphers,

nettle\_get\_hashes and nettle\_get\_armors. Test

vectors for hashes and hmac.

Nippon Telegraph and Telephone Corporation

LGPL:ed reference implementation of the

Camellia cipher.

Andrew M. (floodyberry)

The poly1305 code nettle's C implementation is

derived from.

Aleksey Kravchenko The gosthash94 implementation in rhash library.

Stefan Metzmacher, Jeremy Allison, Michael Adam

Contributed to the CMAC code, which was added

to Nettle by Nikos Mavroyanopoulos.

Nikos Mavroyanopoulos GCM implementation, RSA blinding code,

interface for general rsa-pkcs1 signatures.

Port of gosthash94 implementation from rhash. Port of

poly1305. Salsa20r12 variant. HKDF (RFC 5869)

implementation. CMAC and SIV-CMAV

implementation. CTR and GCM optimizations.

Implementation of versioned symbols. Setup of

.gitlab-ci.yml. Large number of smaller fixes.

Andres Mejia Ported Ripemd160 from libgcrypt.

Martin Storsjö Implemented m4 macrology to make x86\_64

assembly files work with the windows ABI.

Several other portability improvements.

Jeronimo Pellegrini Documentation for base16 and base64 functions.

Tim Ruehsen Several smaller cleanups and bugfixes.

Fredrik Thulin Test vectors for pbkdf2-hmac-sha512.

Joachim Strömbergson Chacha implementation. Support for sha512\_224

and sha512\_256.

Owen Kirby Implementation of CCM mode.

Amos Jeffries Implementation of base64url encoding.

Daiki Ueno Implementation of RSA-PSS signatures,

curve448, shake256, ed448-shake256 signatures,

chacha functions for 32-bit nonce, struct

nettle\_mac interface, siv-gcm.

Dmitry Baryshkov CFB and CFB8 modes, CMAC64. gosthash94cp and

Streebog hash functions, GOST DSA signatures

and curves GC256B and GC512A. Various bug

fixes and cleanups.

Simo Sorce Side-channel silent RSA functions. XTS

implementation.

H.J. Lu Assembly annotations for Intel "Control-flow

Enforcement Technology".

Stephen R. van den Berg

Port of bcrypt.

Mamone Tarsha Kurdi Powerpc64 assembly and fat build setup,

including AES and GCM. Arm64 assembly and fat

build setup, including AES, Chacha, GCM, SHA1,

SHA256. S390x assembly and fat build setup,

including AES, Chacha, memxor, memxor3, SHA1,

SHA256, SHA512, SHA3.

Nicolas Mora RFC 3394 keywrap.

Tianjia Zhang SM3 hash function, SM4 block cipher.

Amitay Isaacs Powerpc64 assembly for secp192r1, secp224r1

and secp256r1.

Martin Schwenke Powerpc64 assembly for secp384r1, secp521r1,

curve25519 and curve448.

Zoltan Fridrich Ballon password hashing.