CycloneCRYPTO

CycloneCRYPTO is a cryptographic toolkit designed for use in embedded systems. It provides a comprehensive set of cryptographic primitives (hash functions, stream and block ciphers, public key cryptography) that can be used to add security features to your embedded application.

Main Features

- Base64 encoding
- MD2, MD4 and MD5 hash functions
- RIPEMD-128 and RIPEMD-160 hash functions
- SHA-1 hash function
- SHA-2 family hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)
- SHA-3 family hash functions (SHA3-224, SHA3-256, SHA3-384 and SHA3-512)
- BLAKE2b family hash functions (BLAKE2b160, BLAKE2b256, BLAKE2b384, BLAKE2b512)
- BLAKE2s family hash functions (BLAKE2s128, BLAKE2s160, BLAKE2s224, BLAKE2s256)
- Tiger/192 hash function
- Whirlpool hash function
- SHAKE128, SHAKE256 and cSHAKE extendable-output functions (XOF)
- Keccak sponge function
- HMAC, CMAC, GMAC, KMAC, XCBC-MAC and Poly1305 message-authentication code
- Supports ChaCha, Salsa20, Trivium and ZUC stream ciphers
- Legacy support for RC4 stream ciphers
- Supports 128-bit block ciphers (RC6, CAST-256, AES, Twofish, MARS, Serpent, Camellia, ARIA, SEED)
- Legacy support for 64-bit block ciphers (RC2, CAST-128, IDEA, DES, 3DES, Blowfish, PRESENT, TEA, XTEA)
- Supports ECB, CBC, CFB, OFB, CTR and XTS operation modes for all symmetric block ciphers
- Cipher Block Chaining-MAC (CCM) and Galois Counter Mode (GCM)
- Synthetic Initialization Vector (SIV) authenticated encryption
- ChaCha20Poly1305 Authenticated Encryption with Associated Data (AEAD)
- Ascon-Based Lightweight Cryptography (Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128, Ascon-CXOF128)
- RSA public key cryptography (PKCS #1 v1.5 and v2.2)
- Digital Signature Algorithm (DSA)
- Diffie-Hellman key exchange (PKCS #3)
- Password-Based Cryptography Standard (PKCS #5)
- Cryptographic Message Syntax (PKCS #7)
- Elliptic Curve Cryptography (ECC)
- Elliptic Curve Diffie-Hellman (ECDH)
- ECDH over Curve25519 and Curve448 elliptic curves (X25519 and X448)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Deterministic ECDSA signature generation
- EdDSA signature scheme (Ed25519 and Ed448 elliptic curves)
- Supports elliptic curves defined over prime fields (NIST-P and Brainpool)
- ShangMi (SM) cryptographic algorithms SM2, SM3 an SM4
- Multiple precision arithmetic library with optimized assembly code (for ARM and MIPS-based MCUs)
- X.509 certificate, CRL and CSR parsing functions
- X.509 certification and CSR generation
- OCSP client (Online Certificate Status Protocol)
- Parsing and formatting of public/private keys (PKCS #1 and PKCS #8 formats supported)
- Parsing of encrypted private keys (PKCS #1 and PKCS #8 formats supported)
- PBKDF1, PBKDF2, HKDF and Concat KDF key derivation functions
- bcrypt, scrypt, MD5-crypt and SHA-crypt password hashing functions
- Hash_DRBG, HMAC_DRBG, CTR_DRBG and XDRBG pseudorandom number generators
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Portable architecture (supports little-endian and big-endian architectures)
- Extensive test suite available on request (for commercial licenses)

RFC

- RFC 1319: The MD2 Message-Digest Algorithm
- RFC 1321: The MD5 Message-Digest Algorithm
- RFC 1423: Privacy Enhancement for Internet Electronic Mail Part III: Algorithms, Modes, and Identifiers
- RFC 2104: HMAC: Keyed-Hashing for Message Authentication
- RFC 2144: The CAST-128 Encryption Algorithm
- RFC 2268: A Description of the RC2 Encryption Algorithm
- RFC 2313: PKCS #1: RSA Encryption Version 1.5
- RFC 2315: PKCS #7: Cryptographic Message Syntax Version 1.5
- RFC 2612: The CAST-256 Encryption Algorithm
- RFC 2631: Diffie-Hellman Key Agreement Method
- RFC 2898: PKCS #5: Password-Based Cryptography Specification Version 2.0
- RFC 2985: PKCS #9: Selected Object Classes and Attribute Types Version 2.0
- RFC 2986: PKCS #10: Certification Request Syntax Specification Version 1.7
- RFC 3174: US Secure Hash Algorithm 1 (SHA1)
- RFC 3447: PKCS #1: RSA Cryptography Specifications Version 2.1
- RFC 4269: The SEED Encryption Algorithm
- RFC 4493: The AES-CMAC Algorithm
- RFC 4648: The Base16, Base32, and Base64 Data Encodings
- RFC 5208: PKCS #8: Private-Key Information Syntax Specification Version 1.2
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 5297: Synthetic Initialization Vector (SIV) Authenticated Encryption Using the AES
- RFC 5639: ECC Brainpool Standard Curves and Curve Generation
- RFC 5794: A Description of the ARIA Encryption Algorithm
- RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)
- RFC 5915: Elliptic Curve Private Key Structure
- RFC 5958: Asymmetric Key Packages
- RFC 6090: Fundamental Elliptic Curve Cryptography Algorithms
- RFC 6229: Test Vectors for the Stream Cipher RC4
- RFC 6234: US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)
- RFC 6979: Deterministic Usage of the DSA and ECDSA
- RFC 6818: Updates to the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)
- RFC 7468: Textual Encodings of PKIX, PKCS, and CMS Structures
- RFC 7539: ChaCha20 and Poly1305 for IETF Protocols
- RFC 7693: The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)
- RFC 7748: Elliptic Curves for Security (Curve25519 and Curve448)
- RFC 7914: The scrypt Password-Based Key Derivation Function
- RFC 8017: PKCS #1: RSA Cryptography Specifications Version 2.2
- RFC 8018: PKCS #5: Password-Based Cryptography Specification Version 2.1
- RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)
- RFC 8410: Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the PKIX
- RFC 8603: Commercial National Security Algorithm (CNSA) Suite Certificate and CRL Profile
- RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension
- RFC 9295: Clarifications for Ed25519, Ed448, X25519, and X448 Algorithm Identifiers
- RFC draft: SM2 Digital Signature Algorithm
- RFC draft: The SM3 Cryptographic Hash Function
- RFC draft: The SM4 Block Cipher Algorithm And Its Modes Of Operations

IEEE

- IEEE Std 1363-2000: Standard Specifications for Public-Key Cryptography

Certicom Research

- SEC 1: Elliptic Curve Cryptography
- SEC 2: Recommended Elliptic Curve Domain Parameters

NIST

- FIPS 46-3: Data Encryption Standard
- FIPS 180-4: Secure Hash Standard (SHS)
- FIPS 186-5: Digital Signature Standard (DSS)
- FIPS 197: Advanced Encryption Standard
- FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)
- FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable Output Functions
- SP 800-38A: Recommendation for Block Cipher Modes of Operation - Methods and Techniques
- SP 800-38C: The CCM Mode for Authentication and Confidentiality
- SP 800-38D: Galois/Counter Mode (GCM) and GMAC
- SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- SP 800-232: Ascon-Based Lightweight Cryptography Standards for Constrained Devices

RSA Laboratories

- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Standard

Supported Processors

- ARM Cortex-M3
- ARM Cortex-M4
- ARM Cortex-M7
- ARM Cortex-M33
- ARM Cortex-M55
- ARM Cortex-M85
- ARM Cortex-R4
- ARM Cortex-A5
- ARM Cortex-A7
- ARM Cortex-A8
- ARM Cortex-A9
- ARM Cortex-A55
- RISC-V
- MIPS M4K
- MIPS microAptiv / M-Class
- Infineon TriCore AURIX
- PowerPC e200
- Coldfire V2
- RX600
- AVR32
- Xtensa LX6

Supported Compilers / Toolchains

Toolchain / IDE	Compiler
Makefile	GCC
AC6 System Workbench for STM32 (SW4STM32)	GCC
Atollic TrueSTUDIO	GCC
Espressif ESP-IDF	GCC
HighTec Toolset for TriCore	GCC
IAR Embedded Workbench	EWARM, EWRX
Infineon DAVE	GCC
Keil MDK-ARM	ARM Compiler v5, ARM Compiler v6 (CLANG)
Microchip Studio (Atmel Studio)	GCC
Microchip MPLAB X	GCC, XC32
Microsoft Visual Studio	MSVC
NXP MCUXpresso	GCC
NXP S32 Design Studio (S32DS)	GCC
Renesas e2Studio	GCC, CC-RX
Segger Embedded Studio	GCC
ST STM32CubeIDE	GCC
Tasking VX-Toolset	VX-Toolset for TriCore
TI Code Composer Studio (CSS)	GCC, ARM-CGT