
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. CycloneCrypto is available either as open source (GPLv2) or under a commercial license.

## Main Features

- Base16/32/64 data encoding
- MD2, MD4, MD5, SHA-1, RIPEMD-128, RIPEMD-128, Tiger/192 and Whirlpooh hash functions
- SHA-2 family hash functions (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 and BLAKE2s family hash functions
- Keccak sponge function
- RC4 and ChaCha stream ciphers
- Block ciphers (RC2, RC6, IDEA, DES, 3DES, AES, Camellia, SEED, ARIA, Present)
- Supports ECB, CBC, CFB, OFB, CTR and XTS cipher modes
- Cipher Block Chaining-MAC (CCM) and Galois Counter Mode (GCM)
- HMAC, CMAC and GMAC message-authentication code
- Poly1305 message-authentication code
- ChaCha20Poly1305 AEAD
- 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)
- HKDF (HMAC-based Key Derivation Function)
- Elliptic Curve Cryptography (ECC)
- Elliptic Curve Diffie-Hellman (ECDH)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Edwards-Curve Digital Signature Algorithm (EdDSA)
- Supports elliptic curves defined over prime fields (NIST-P and Brainpool)
- Supports Curve25519, Curve448, Ed25519 and Ed448 elliptic curves
- Multiple precision arithmetic library with optimized assembly code (for ARM® and MIPS™-based microcontrollers)
- X.509 certificate parsing functions
- Supports hardware accelerated encryption engines (when available)
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Portable architecture (supports little-endian and big-endian architectures)
- The library is distributed as a full ANSI C and highly maintainable source code
- Dual licensing (open source or commercial license)
- Extensive test suite available on request (for commercial licenses)

## Supported Devices

- ARM7TDMI®
- ARM926EJ-S™
- Cortex™-M3/M4/M7
- Cortex™-A5/A8/A9
- APS1 / APS3 / APS3R / APS5 / FPS6
- AVR32
- PIC32
- RX600
- Xtensa LX6

## Related products

- CycloneTCP (dual IPv4/IPv6 stack dedicated to embedded applications)
- CycloneSSL (lightweight SSL/TLS library)

## Reference Standards

### *RFC*

- RFC 4648: The Base16, Base32, and Base64 Data Encodings
- RFC 1319: The MD2 Message-Digest Algorithm
- RFC 1321: The MD5 Message-Digest Algorithm
- RFC 2104: HMAC: Keyed-Hashing for Message Authentication
- RFC 4269: The SEED Encryption Algorithm
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 5794: A Description of the ARIA Encryption Algorithm
- RFC 5639: ECC Brainpool Standard Curves and Curve Generation
- RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)
- RFC 6090: Fundamental Elliptic Curve Cryptography Algorithms
- RFC 7748: Elliptic Curves for Security (Curve25519 and Curve448)
- RFC 7539: ChaCha20 and Poly1305 for IETF Protocols
- RFC 7693: The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)
- RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)

### *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
- GEC 2: Test Vectors for SEC 1

### *NIST*

- FIPS 46-3: Data Encryption Standard
- FIPS 180-4: Secure Hash Standard
- FIPS 186-3: 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: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
- SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
- SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

### *RSA Laboratories*

- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard



 