



# wolfCrypt Embedded Crypto Engine

## Description

The wolfCrypt cryptography engine is a lightweight crypto library written in ANSI C and targeted for embedded and RTOS environments - primarily because of its small size, speed, and feature set. It is commonly used in standard operating environments as well because of its royalty-free pricing and excellent cross platform support. wolfCrypt supports the most popular algorithms and ciphers as well as progressive ones such as HC-128, RABBIT, NTRU, ChaCha, and Poly1305. wolfCrypt is stable, production-ready, and backed by an excellent support team. It is used in millions of application and devices worldwide.

wolfCrypt is built for maximum portability and is generally very easy to compile on new platforms. It supports the C programming language as a primary interface. If your desired platform is not listed under the supported operating environments, or you have interest in using wolfCrypt in another programming language not currently supported, please contact wolfSSL.

The wolfCrypt module is now **FIPS 140-2 Level 1 validated**, with certificate #2425. For additional information, visit our FIPS FAQ page or contact [fips@wolfssl.com](mailto:fips@wolfssl.com).

## Features

- Multiple Hashing Functions:  
MD2, MD4, MD5, SHA-1, SHA-2 (SHA-256, SHA-224, SHA-384, SHA-512), Blake2b, RIPEMD-160, Poly1305
- Block, Stream, and Authenticated Ciphers:  
AES (CBC, CTR, GCM, CCM, GMAC, CMAC), Camellia, DES, 3DES, ARC4, RABBIT, HC-128, ChaCha20
- Public Key Options:  
RSA, DSS, DH, ECDH, ECDH-ECDSA, ECDHE-ECDSA, ECDH-RSA, ECDHE-RSA, NTRU
- Password-based Key Derivation:  
HMAC, PBKDF2, PKCS#5
- Ed25519/Curve 25519
- Hash-based PRNG
- X.509 Encoding / Decoding
- RSA and ECC Key Generation
- X.509 v3 Signed Certificate Generation
- PKCS #1, #5, #8, #12 Private Key Encryption
- PKCS #7 Cryptographic Message Syntax
- PCKS #10 Certificate Signing Request
- Assembly Optimizations
- Custom Memory Hooks / Simple API's
- Easily ties into Hardware-based RNG solutions
- Hardware Crypto Support  
Intel AES-NI, AVX1/2, RDRAND, RDSEED, SGX, Cavium NITROX, Intel QuickAssist, STM32F2/F4, NXP (CAU, mmCAU, SEC, LTC), Microchip PIC32MZ, ARMv8
- OpenSSL compatibility layer

## Supported Chipmakers

- wolfCrypt has support for chipsets including ARM, Intel, Motorola, mbed, NXP/Freescale, Microchip (PIC32)/Atmel, STMicro (STM32F2/F4), Analog Devices, Texas Instruments, and more.
- If you would like to use or test wolfSSL on another chipset, let us know and we'll be happy to support you.

## Supported Operating Environments

- Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, TRON/ITRON/ $\mu$ ITRON, Micrium's  $\mu$ C/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, TI-RTOS, uTasker, embOS
- If you would like to test wolfSSL on another environment, let us know and we'll be happy to support you.