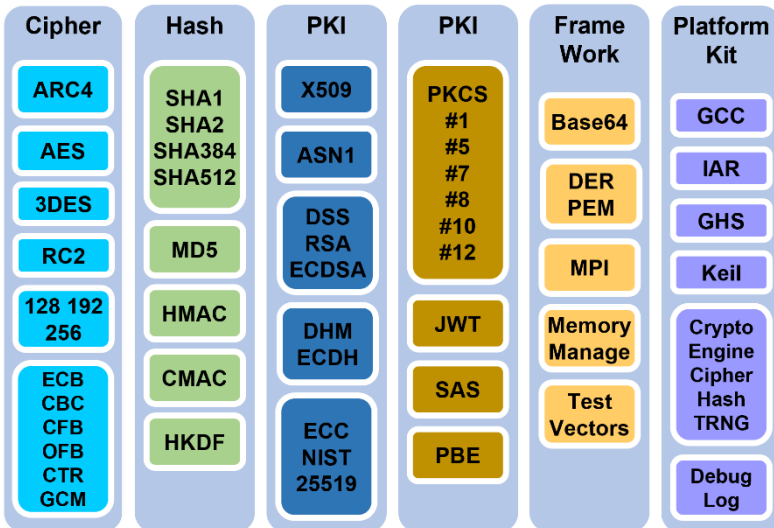


### Overview

Add electronic data privacy, authentication, and integrity to your product. The Cypherbridge Systems uCrypt Toolkit can be used for a wide variety of applications such as stream and block ciphers, hashing, RSA asymmetric raw key, file-based encryption, and PKI based authentication.

uCrypt is a compact ANSI C software library for cryptographic and hash processing, targeted for small and medium memory models where CPU, RAM and flash resources are carefully allocated and balanced. The uCrypt Library uses a proven non-threaded, run-to-completion synchronous execution design for fast, efficient cryptographic operations.

The uCrypt library is integrated with the Cypherbridge Systems SDKPac, including uSSL and uLoadXL secure boot loader. This offers an upgrade path to a full-function TLS network based encryption solution for data-in-flight, secure file transfer, OTA update, and more.



### Supported Standards and Features

uCrypt implements standards based algorithms including:

- ✓ Symmetric: Stream Ciphers: RC4, Block Ciphers: DES & 3DES (FIPS 46-3) ECB & CBC, AES ECB CBC CFB CTR GCM
- ✓ PKI Asymmetric Algorithms: Encryption: RSA (PKCS #1); Elliptic Curve Integrated Encryption Scheme (ANSI X9.63-2001/IEEE P1363); Digital Signatures: DSS (FIPS 186-2);
- ✓ Message Digest (Hashing) Algorithms: SHA1 (FIPS 180-1), SHA-256, SHA-384, and SHA-512 (FIPS 180-2); MD5; HMAC-SHA
- ✓ Key Agreement Algorithms: Diffie-Hellman (PKCS #3 v1.4); Elliptic Curve Diffie-Hellman (ANSI X9.63)
- ✓ ARM PSA API framework
- ✓ Platform adaptive HW interface including RNG interface for TRNG

### Features

- ✓ Commercial grade standards based cryptographic algorithms
- ✓ X.509 PKI processing
- ✓ Integrated framework includes integrated memory manager, and full self-test examples to integrate with your application
- ✓ Platform kit interfaces to run-time resources
- ✓ Optional hardware engine acceleration seamlessly switches between software and hardware.
- ✓ Hardware engine yields faster throughput and lower memory footprint
- ✓ Diagnostic trace log output for debug and support
- ✓ Lightweight ANSI C toolkit has compact footprint for embedded systems
- ✓ Thread-free and RTOS independent
- ✓ Supports IAR, Keil, GCC, and Green Hills MULTI toolchains
- ✓ Integrated on wide range of off the shelf development kits and 32- and 64-bit systems, including RTOS, INTEGRITY, and x86\_64

### For Pricing and Availability

Cypherbridge Systems, LLC  
 7040 Avenida Encinas #104211  
 Carlsbad CA 92011 USA +1 (760) 814-1575  
[www.cypherbridge.com](http://www.cypherbridge.com)  
[sales@cypherbridge.com](mailto:sales@cypherbridge.com)

CSL-uCrypt-231211-A

Copyright © 2023 Cypherbridge Systems, LLC  
 Features & specifications can change without notice  
 Cypherbridge® is a registered trademark  
 uCrypt™ is a trademark of Cypherbridge Systems  
 LLC All Rights Reserved