Karel Miko / CryptX-0.088

53 ++ ⭐ Starred 36

Changes for version 0.088 - 2026-04-23

- Crypt::KeyDerivation - new functions: pbkdf1_openssl, bcrypt_pbkdf, scrypt_pbkdf, argon2_pbkdf
- Crypt::Misc - new functions: random_v7uuid, is_uuid
- bundled libtomcrypt update branch:develop (commit: 2e441a17 2026-04-15)
- bundled libtommath update branch:develop (commit: ae40a87 2026-04-20)
- security fix CVE-2026-41564 https://github.com/DCIT/perl-CryptX/security/advisories/GHSA-24c2-gp6c-24c6

Documentation

README.md
SECURITY.md

Modules

Crypt::AuthEnc	[internal only]
Crypt::AuthEnc::CCM	Authenticated encryption in CCM mode
Crypt::AuthEnc::ChaCha20Poly1305	Authenticated encryption in ChaCha20-Poly1305 mode
Crypt::AuthEnc::EAX	Authenticated encryption in EAX mode
Crypt::AuthEnc::GCM	Authenticated encryption in GCM mode
Crypt::AuthEnc::OCB	Authenticated encryption in OCBv3 mode
Crypt::Checksum	[internal only]
Crypt::Checksum::Adler32	Compute Adler32 checksum
Crypt::Checksum::CRC32	Compute CRC32 checksum
Crypt::Cipher	Generic interface to cipher functions
Crypt::Cipher::AES	Symmetric cipher AES (aka Rijndael), key size: 128/192/256 bits
Crypt::Cipher::Anubis	Symmetric cipher Anubis, key size: 128-320 bits
Crypt::Cipher::Blowfish	Symmetric cipher Blowfish, key size: 64-576 bits
Crypt::Cipher::CAST5	Symmetric cipher CAST5 (aka CAST-128), key size: 40-128 bits
Crypt::Cipher::Camellia	Symmetric cipher Camellia, key size: 128/192/256 bits

	3DES), key size: 192[168] bits
Crypt::Cipher::IDEA	Symmetric cipher IDEA, key size: 128 bits
Crypt::Cipher::KASUMI	Symmetric cipher KASUMI, key size: 128 bits
Crypt::Cipher::Khazad	Symmetric cipher Khazad, key size: 128 bits
Crypt::Cipher::MULTI2	Symmetric cipher MULTI2, key size: 320 bits
Crypt::Cipher::Noekeon	Symmetric cipher Noekeon, key size: 128 bits
Crypt::Cipher::RC2	Symmetric cipher RC2, key size: 40-1024 bits
Crypt::Cipher::RC5	Symmetric cipher RC5, key size: 64-1024 bits
Crypt::Cipher::RC6	Symmetric cipher RC6, key size: 64-1024 bits
Crypt::Cipher::SAFERP	Symmetric cipher SAFER+, key size: 128/192/256 bits
Crypt::Cipher::SAFER_K128	Symmetric cipher SAFER_K128, key size: 128 bits
Crypt::Cipher::SAFER_K64	Symmetric cipher SAFER_K64, key size: 64 bits
Crypt::Cipher::SAFER_SK128	Symmetric cipher SAFER_SK128, key size: 128 bits
Crypt::Cipher::SAFER_SK64	Symmetric cipher SAFER_SK64, key size: 64 bits
Crypt::Cipher::SEED	Symmetric cipher SEED, key size: 128 bits
Crypt::Cipher::Serpent	Symmetric cipher Serpent, key size: 128/192/256 bits
Crypt::Cipher::Skipjack	Symmetric cipher Skipjack, key size: 80 bits
Crypt::Cipher::Twofish	Symmetric cipher Twofish, key size: 128/192/256 bits
Crypt::Cipher::XTEA	Symmetric cipher XTEA, key size: 128 bits
Crypt::Digest	Generic interface to hash/digest functions
Crypt::Digest::BLAKE2b_160	Hash function BLAKE2b [size: 160 bits]
Crypt::Digest::BLAKE2b_256	Hash function BLAKE2b [size: 256 bits]
Crypt::Digest::BLAKE2b_384	Hash function BLAKE2b [size: 384 bits]
Crypt::Digest::BLAKE2b_512	Hash function BLAKE2b [size: 512 bits]
Crypt::Digest::BLAKE2s_128	Hash function BLAKE2s [size: 128 bits]
Crypt::Digest::BLAKE2s_160	Hash function BLAKE2s [size: 160 bits]
Crypt::Digest::BLAKE2s_224	Hash function BLAKE2s [size: 224 bits]
Crypt::Digest::BLAKE2s_256	Hash function BLAKE2s [size: 256 bits]
Crypt::Digest::CHAES	Hash function - CipherHash based on AES [size: 128 bits]
Crypt::Digest::Keccak224	Hash function Keccak-224 [size: 224 bits]
Crypt::Digest::Keccak256	Hash function Keccak-256 [size: 256 bits]
Crypt::Digest::Keccak384	Hash function Keccak-384 [size: 384 bits]
Crypt::Digest::Keccak512	Hash function Keccak-512 [size: 512 bits]
Crypt::Digest::MD2	Hash function MD2 [size: 128 bits]
Crypt::Digest::MD4	Hash function MD4 [size: 128 bits]
Crypt::Digest::MD5	Hash function MD5 [size: 128 bits]

Crypt::Digest::RIPEMD256	Hash function RIPEMD-256 [size: 256 bits]
Crypt::Digest::RIPEMD320	Hash function RIPEMD-320 [size: 320 bits]
Crypt::Digest::SHA1	Hash function SHA-1 [size: 160 bits]
Crypt::Digest::SHA224	Hash function SHA-224 [size: 224 bits]
Crypt::Digest::SHA256	Hash function SHA-256 [size: 256 bits]
Crypt::Digest::SHA384	Hash function SHA-384 [size: 384 bits]
Crypt::Digest::SHA3_224	Hash function SHA3-224 [size: 224 bits]
Crypt::Digest::SHA3_256	Hash function SHA3-256 [size: 256 bits]
Crypt::Digest::SHA3_384	Hash function SHA3-384 [size: 384 bits]
Crypt::Digest::SHA3_512	Hash function SHA3-512 [size: 512 bits]
Crypt::Digest::SHA512	Hash function SHA-512 [size: 512 bits]
Crypt::Digest::SHA512_224	Hash function SHA-512/224 [size: 224 bits]
Crypt::Digest::SHA512_256	Hash function SHA-512/256 [size: 256 bits]
Crypt::Digest::SHAKE	Hash functions SHAKE128, SHAKE256 from SHA3 family
Crypt::Digest::Tiger192	Hash function Tiger-192 [size: 192 bits]
Crypt::Digest::Whirlpool	Hash function Whirlpool [size: 512 bits]
Crypt::KeyDerivation	PBKDF1, PBKDF2, HKDF, Bcrypt, Scrypt, Argon2 key derivation functions
Crypt::Mac	[internal only]
Crypt::Mac::BLAKE2b	Message authentication code BLAKE2b MAC (RFC 7693)
Crypt::Mac::BLAKE2s	Message authentication code BLAKE2s MAC (RFC 7693)
Crypt::Mac::F9	Message authentication code F9
Crypt::Mac::HMAC	Message authentication code HMAC
Crypt::Mac::OMAC	Message authentication code OMAC
Crypt::Mac::PMAC	Message authentication code PMAC
Crypt::Mac::Pelican	Message authentication code Pelican (AES based MAC)
Crypt::Mac::Poly1305	Message authentication code Poly1305 (RFC 7539)
Crypt::Mac::XCBC	Message authentication code XCBC (RFC 3566)
Crypt::Misc	miscellaneous functions related to (or used by) CryptX
Crypt::Mode	[internal only]
Crypt::Mode::CBC	Block cipher mode CBC [Cipher-block chaining]
Crypt::Mode::CFB	Block cipher mode CFB [Cipher feedback]
Crypt::Mode::CTR	Block cipher mode CTR [Counter mode]
Crypt::Mode::ECB	Block cipher mode ECB [Electronic codebook]
Crypt::Mode::OFB	Block cipher mode OFB [Output feedback]

Crypt::PK::DSA	Public key cryptography based on DSA
Crypt::PK::ECC	Public key cryptography based on EC
Crypt::PK::Ed25519	Digital signature based on Ed25519
Crypt::PK::RSA	Public key cryptography based on RSA
Crypt::PK::X25519	Asymmetric cryptography based on X25519
Crypt::PRNG	Cryptographically secure random number generator
Crypt::PRNG::ChaCha20	Cryptographically secure PRNG based on ChaCha20 (stream cipher) algorithm
Crypt::PRNG::Fortuna	Cryptographically secure PRNG based on Fortuna algorithm
Crypt::PRNG::RC4	Cryptographically secure PRNG based on RC4 (stream cipher) algorithm
Crypt::PRNG::Sober128	Cryptographically secure PRNG based on Sober128 (stream cipher) algorithm
Crypt::PRNG::Yarrow	Cryptographically secure PRNG based on Yarrow algorithm
Crypt::Stream::ChaCha	Stream cipher ChaCha
Crypt::Stream::RC4	Stream cipher RC4
Crypt::Stream::Rabbit	Stream cipher Rabbit
Crypt::Stream::Salsa20	Stream cipher Salsa20
Crypt::Stream::Sober128	Stream cipher Sober128
Crypt::Stream::Sosemanuk	Stream cipher Sosemanuk
CryptX	Cryptographic toolkit
Math::BigInt::LTM	Use the libtommath library for Math::BigInt routines

Other files

Changes
LICENSE
MANIFEST
META.json
META.yml
Makefile.PL