

Comparison of Python cryptography modules

	M2Crypto	pycryptopp	cryptlib_py	python-nss	pycrypto	cryptopy
Version	0.20.2	0.5.17	3.2.2	0.8	2.0.1	1.2.5
Date	October 7, 2009	September 23, 2009	September 13, 2005	September 21, 2009	June 14, 2005	March 3, 2003
License	BSD-style	GPL	GPL-like ¹ , Commercial ²	MPLv1.1 ³	Public Domain	Artistic License
Export Laws	USA	USA	New Zealand	USA	USA	USA
Type	Wrapper	Wrapper	Wrapper	Wrapper	C module	Pure Python
Underlying system	OpenSSL	Crypto++ ⁴	Cryptlib	NSS	N/A	N/A
Platform	CPython ⁵	CPython	CPython	Cpython on Linux	CPython	Any
Python	<= 2.6	<= 2.5	2.x ⁶	= 2.6	<= 2.6	2.2+
Binaries	Linux, Windows, Mac OS X	Linux	Windows	Fedora Linux/RHEL	Linux	N/A
Higher level API	Some	No	Full	Some	No	Some
Extensions	Loadable “engines” (shared libraries)	Not supported	Statically compiled C modules	Not supported	Not supported	Python modules

Technical details

	M2Crypto	pycryptopp	cryptlib_py	python-nss	pycrypto	cryptopy
Symmetric Ciphers	Blowfish, CAST, CAST5, DES, Triple DES, IDEA, RC2, RC4, RC5, AES, Camellia, SEED	AES (Rijndael)	AES, Blowfish, CAST-128, DES, Triple DES, IDEA, RC2, RC4, RC5 Skipjack	AES, DES, Triple DES, RC4, RC2	AES, RC2, RC4, RC5, Blowfish, CAST, DES, Triple DES, IDEA, XOR	Rijndael, AES, RC4, WEP, TKIP
Asymmetric	DSA, RSA, Elliptic Curve DSA, GOST R 34.10 1994/2001	RSA	DSA, Elgamal, RSA	RSA, DSA, Elliptic Curve DSA	DSA, Elgamal, RSA	-
Key Agreement	Diffie-Hellman, Elliptic Curve Diffie-Hellman (ECDH)	-	Diffie-Hellman	RSA, Diffie-Hellman, Elliptic Curve Diffie-Hellman (ECDH)	-	-
Hashes	MD2, MD4, MD5, MDC2, RIPEMD-160, SHA-1, SHA-224/256/384/512	SHA-256	MD2, MD4, MD5, RIPEMD-160, SHA-1, SHA-2/SHA-256	SHA-1/SHA-256/SHA-384/SHA-512, MD5, MD2	MD2, MD4, MD5, RIPEMD, SHA, SHA-256	MD5, SHA-1
Message Authentication	HMAC, GOST 28147-89 MAC	-	HMAC-MD5, HMAC-SHA, HMAC-RIPEMD-160	HMAC	HMAC	HMAC, IEEE
RNG	Custom ⁷ algorithm based on SHA-1	ANSI X9.17 appendix C, RandomPool	/dev/random, EGD, PRNGD, ANSI X9.17/X9.31, hardware generators	FIPS 186-2	Randpool	Rijndael_256k_256b
Certificates, I/O and Encoding	X509, X509v3, ASN.1, PEM, S/MIME, PKCS#7, PKCS#12	-	X.509v1 to X.509v4, SET, S/MIME, PGP/OpenPGP, AuthentiCode, Identrus, SigG, Qualified Certificates, IPSec, PKCS#7, PKCS#11, PKCS#15	PKCS#5, #3, #5, #7, #8, #9, #10, #11, #12, S/MIME, X.509v3, OCSP	RFC1751	-
Supported Hardware	Through custom “engines”	-	PKCS#11 compatible, other	PKCS#11 compatible	-	-

Certification

	M2Crypto	pycryptopp	cryptlib_py	python-nss	pycrypto	cryptopy
FIPS-140	Level 2 ⁸	Level 2	Yes ⁹	Level 2	No	No
ITSEC/Common Criteria	No	No	Yes	No	No	No
NSA Suite B	No	No	No	No	No	No

¹ The package itself is Public Domain; the underlying system, however, is under dual GPL/Commercial license

² NZ\$20,000 for the Source Code License

³ Mozilla Public License

⁴ Only a fraction of the underlying Crypto++ functionality is exposed at the Python level

⁵ Any platforms where CPython is available

⁶ Supposedly (no info on the site)

⁷ No, you can't replace it

⁸ FIPS validation support is included in some support plans

⁹ Level is not specified