Crypto++ 7.0.0 Benchmarks

Here are speed benchmarks for some commonly used cryptographic algorithms.

CPU frequency of the test platform was not provided.

Algorithm	MiB/Second
NonblockingRng	190
AutoSeededRandomPool	234
AutoSeededX917RNG(AES)	28
MT19937	582
RDRAND	67
RDSEED	21
AES/OFB RNG	970
Hash_DRBG(SHA1)	65
Hash_DRBG(SHA256)	77
HMAC_DRBG(SHA1)	16
HMAC_DRBG(SHA256)	19
CRC32	574
CRC32C	4823
Adler32	2465
MD5	659
SHA-1	579
SHA-256	314
SHA-512	392
SHA3-224	316
SHA3-256	299
SHA3-384	228
SHA3-512	159
Keccak-224	315
Keccak-256	300
Keccak-384	229
Keccak-512	159
Tiger	618
Whirlpool	163
RIPEMD-160	255
RIPEMD-320	281
RIPEMD-128	437
RIPEMD-256	497
SM3	258
BLAKE2s	614
BLAKE2b	871

Algorithm	MiB/Second	Microseconds to Setup Key and IV
GMAC(AES)	6349	0.695
VMAC(AES)-64 (128-bit key)	10505	0.894
VMAC(AES)-128 (128-bit key)	6322	0.977
HMAC(SHA-1) (128-bit key)	577	1.547
HMAC(SHA-256) (128-bit key)	312	1.538
Two-Track-MAC (160-bit key)	279	0.035
CMAC(AES) (128-bit key)	1194	0.233
DMAC(AES) (128-bit key)	1201	0.669
Poly1305(AES) (256-bit key)	1159	0.318
BLAKE2s (256-bit key)	613	0.341
BLAKE2b (512-bit key)	866	0.341
SipHash-2-4 (128-bit key)	1818	0.044
SipHash-4-8 (128-bit key)	1048	0.044
Panama-LE (256-bit key)	1986	0.785
Panama-BE (256-bit key)	932	1.081
Salsa20 (256-bit key)	1073	0.355
Salsa20/12	1656	0.406
Salsa20/8	2292	0.404
ChaCha20 (256-bit key)	516	0.278
ChaCha12 (256-bit key)	752	0.278
ChaCha8 (256-bit key)	993	0.278
Sosemanuk (128-bit key)	1868	0.536
MARC4 (128-bit key)	662	0.815
SEAL-3.0-LE (160-bit key)	810	21.249
WAKE-OFB-LE (256-bit key)	450	1.369
AES/CTR (128-bit key)	4312	0.508
AES/CTR (192-bit key)	3745	0.500
AES/CTR (256-bit key)	3298	0.518
AES/CBC (128-bit key)	1180	0.405
AES/CBC (192-bit key)	1037	0.384
AES/CBC (256-bit key)	909	0.406
AES/OFB (128-bit key)	1083	0.521
AES/CFB (128-bit key)	1131	0.538
AES/ECB (128-bit key)	5412	0.140
ARIA/CTR (128-bit key)	149	0.511
ARIA/CTR (256-bit key)	117	0.524
Camellia/CTR (128-bit key)	160	0.491
Camellia/CTR (256-bit key)	126	0.507
Twofish/CTR (128-bit key)	199	1.847
Threefish-256(256)/CTR (256-bit key)	410	0.555

Algorithm	MiB/Second	Microseconds to Setup Key and IV
Threefish-512(512)/CTR (512-bit key)	531	0.564
Threefish-1024(1024)/CTR (1024-bit key)	328	0.571
Serpent/CTR (128-bit key)	97	0.672
CAST-128/CTR (128-bit key)	122	0.575
CAST-256/CTR (128-bit key)	121	1.167
RC6/CTR (128-bit key)	160	1.891
MARS/CTR (128-bit key)	159	1.048
SHACAL-2/CTR (128-bit key)	201	0.546
SHACAL-2/CTR (512-bit key)	201	0.560
DES/CTR (64-bit key)	85	1.941
DES-XEX3/CTR (192-bit key)	72	1.942
DES-EDE3/CTR (192-bit key)	33	7.988
IDEA/CTR (128-bit key)	99	0.511
RC5 (r=16)	140	1.677
Blowfish/CTR (128-bit key)	140	26.842
TEA/CTR (128-bit key)	77	0.516
XTEA/CTR (128-bit key)	67	0.518
SKIPJACK/CTR (80-bit key)	44	1.840
SEED/CTR (1/2 K table)	70	0.521
SM4/CTR (128-bit key)	98	0.619
Kalyna-128(128)/CTR (128-bit key)	150	0.554
Kalyna-128(256)/CTR (256-bit key)	117	0.594
Kalyna-256(256)/CTR (256-bit key)	152	0.721
Kalyna-256(512)/CTR (512-bit key)	116	0.779
Kalyna-512(512)/CTR (512-bit key)	156	1.024
SIMON-64(96)/CTR (96-bit key)	511	0.486
SIMON-64(128)/CTR (128-bit key)	495	0.498
SIMON-128(128)/CTR (128-bit key)	375	0.511
SIMON-128(192)/CTR (192-bit key)	364	0.508
SIMON-128(256)/CTR (256-bit key)	356	0.531
SPECK-64(96)/CTR (96-bit key)	1286	0.466
SPECK-64(128)/CTR (128-bit key)	1244	0.466
SPECK-128(128)/CTR (128-bit key)	1287	0.475
SPECK-128(192)/CTR (192-bit key)	1205	0.472
SPECK-128(256)/CTR (256-bit key)	1177	0.472
AES/GCM	2490	0.695
AES/CCM (128-bit key)	908	0.625
AES/EAX (128-bit key)	897	0.961

Operation	Milliseconds/Operation
RSA 1024 Encryption	0.03

Operation	Milliseconds/Operation
RSA 1024 Decryption	0.34
LUC 1024 Encryption	0.03
LUC 1024 Decryption	0.54
DLIES 1024 Encryption	0.18
DLIES 1024 Encryption with precomputation	0.38
DLIES 1024 Decryption	0.28
LUCELG 512 Encryption	0.13
LUCELG 512 Encryption with precomputation	0.13
LUCELG 512 Decryption	0.16
RSA 2048 Encryption	0.06
RSA 2048 Decryption	1.19
LUC 2048 Encryption	0.06
LUC 2048 Decryption	1.93
DLIES 2048 Encryption	0.76
DLIES 2048 Encryption with precomputation	0.95
DLIES 2048 Decryption	0.79
LUCELG 1024 Encryption	0.36
LUCELG 1024 Encryption with precomputation	0.37
LUCELG 1024 Decryption	0.36
RSA 1024 Signature	0.34
RSA 1024 Verification	0.03
RW 1024 Signature	0.36
RW 1024 Signature with precomputation	0.36
RW 1024 Verification	0.02
LUC 1024 Signature	0.54
LUC 1024 Verification	0.03
NR 1024 Signature	0.09
NR 1024 Signature with precomputation	0.12
NR 1024 Verification	0.10
NR 1024 Verification with precomputation	0.20
DSA 1024 Signature	0.09
DSA 1024 Signature with precomputation	0.12
DSA 1024 Verification	0.10
DSA 1024 Verification with precomputation	0.19
LUC-HMP 512 Signature	0.12
LUC-HMP 512 Signature with precomputation	0.12
LUC-HMP 512 Verification	0.13
LUC-HMP 512 Verification with precomputation	0.13
ESIGN 1023 Signature	0.07
ESIGN 1023 Verification	0.03
ESIGN 1536 Signature	0.11
ESIGN 1536 Verification	0.04

Operation	Milliseconds/Operation
RSA 2048 Signature	1.18
RSA 2048 Verification	0.06
RW 2048 Signature	1.24
RW 2048 Signature with precomputation	1.24
RW 2048 Verification	0.05
LUC 2048 Signature	1.89
LUC 2048 Verification	0.06
NR 2048 Signature	0.36
NR 2048 Signature with precomputation	0.22
NR 2048 Verification	0.41
NR 2048 Verification with precomputation	0.36
LUC-HMP 1024 Signature	0.35
LUC-HMP 1024 Signature with precomputation	0.35
LUC-HMP 1024 Verification	0.37
LUC-HMP 1024 Verification with precomputation	0.37
ESIGN 2046 Signature	0.13
ESIGN 2046 Verification	0.05
XTR-DH 171 Key-Pair Generation	0.22
XTR-DH 171 Key Agreement	0.43
XTR-DH 342 Key-Pair Generation	0.40
XTR-DH 342 Key Agreement	0.78
DH 1024 Key-Pair Generation	0.11
DH 1024 Key-Pair Generation with precomputation	0.21
DH 1024 Key Agreement	0.29
DH 2048 Key-Pair Generation	0.41
DH 2048 Key-Pair Generation with precomputation	0.51
DH 2048 Key Agreement	0.82
LUCDIF 512 Key-Pair Generation	0.08
LUCDIF 512 Key-Pair Generation with precomputation	0.08
LUCDIF 512 Key Agreement	0.16
LUCDIF 1024 Key-Pair Generation	0.20
LUCDIF 1024 Key-Pair Generation with precomputation	0.20
LUCDIF 1024 Key Agreement	0.38
MQV 1024 Key-Pair Generation	0.09
MQV 1024 Key-Pair Generation with precomputation	0.11
MQV 1024 Key Agreement	0.20
MQV 2048 Key-Pair Generation	0.36
MQV 2048 Key-Pair Generation with precomputation	0.22
MQV 2048 Key Agreement	0.73
ECIES over GF(p) 256 Encryption	1.66
ECIES over GF(p) 256 Encryption with precomputation	1.22
ECIES over GF(p) 256 Decryption	1.13

Operation	Milliseconds/Operation
ECDSA over GF(p) 256 Signature	0.85
ECDSA over GF(p) 256 Signature with precomputation	0.62
ECDSA over GF(p) 256 Verification	2.35
ECDSA over GF(p) 256 Verification with precomputation	1.05
ECDSA-RFC6979 over GF(p) 256 Signature	0.88
ECDSA-RFC6979 over GF(p) 256 Signature with precomputation	0.65
ECDSA-RFC6979 over GF(p) 256 Verification	2.38
ECDSA-RFC6979 over GF(p) 256 Verification with precomputation	1.08
ECGDSA over GF(p) 256 Signature	1.65
ECGDSA over GF(p) 256 Signature with precomputation	1.21
ECGDSA over GF(p) 256 Verification	2.40
ECGDSA over GF(p) 256 Verification with precomputation	1.06
ECDHC over GF(p) 256 Key-Pair Generation	0.83
ECDHC over GF(p) 256 Key-Pair Generation with precomputation	0.61
ECDHC over GF(p) 256 Key Agreement	0.83
ECMQVC over GF(p) 256 Key-Pair Generation	0.82
ECMQVC over GF(p) 256 Key-Pair Generation with precomputation	0.61
ECMQVC over GF(p) 256 Key Agreement	2.38
ECIES over GF(2^n) 233 Encryption	6.37
ECIES over GF(2^n) 233 Encryption with precomputation	1.89
ECIES over GF(2^n) 233 Decryption	3.82
ECDSA over GF(2^n) 233 Signature	3.22
ECDSA over GF(2^n) 233 Signature with precomputation	0.96
ECDSA over GF(2^n) 233 Verification	3.95
ECDSA over GF(2^n) 233 Verification with precomputation	1.63
ECDSA-RFC6979 over GF(2^n) 233 Signature	3.19
ECDSA-RFC6979 over GF(2^n) 233 Signature with precomputation	1.00
ECDSA-RFC6979 over GF(2^n) 233 Verification	3.94
ECDSA-RFC6979 over GF(2^n) 233 Verification with precomputation	1.61
ECGDSA over GF(2^n) 233 Signature	6.41
ECGDSA over GF(2^n) 233 Signature with precomputation	1.92
ECGDSA over GF(2^n) 233 Verification	3.97
ECGDSA over GF(2^n) 233 Verification with precomputation	1.70
ECDHC over GF(2^n) 233 Key-Pair Generation	3.19
ECDHC over GF(2^n) 233 Key-Pair Generation with precomputation	0.95
ECDHC over GF(2^n) 233 Key Agreement	3.25
ECMQVC over GF(2^n) 233 Key-Pair Generation	3.23
ECMQVC over GF(2^n) 233 Key-Pair Generation with precomputation	0.95

Operation	Milliseconds/Operation
ECMQVC over GF(2^n) 233 Key Agreement	4.07

Throughput Geometric Average: 1014.970799

Test started at Mon Sep 30 11:33:06 2019
Test ended at Mon Sep 30 11:38:19 2019