From: maro@isl.ntt.co.jp
To: AESFirstRound@nist.gov
Subject: Java Performance of AES Candidates
Date: Fri, 16 Apr 1999 01:59:34 JST
Sender: maro@sucaba.isl.ntt.co.jp

Dear Director/ITL,

I submit the report titled
  Java Performance of AES Candidates
using PostScript. The file is generated with gzip and
uuencode. If you cannot print the file, please ask me.

Best regards,

/ NTT Laboratories
/ AOKI, Kazumaro
/ E-mail: maro@isl.ntt.co.jp

Java Performance of AES Candidates

NTT Laboratories*

April 15, 1999

1 Introduction

We measured the speeds of the Java implementations of all fifteen AES candidates and DES on various computers with various Java virtual machines.

2 Environments

We measured the speeds for fifteen combinations of computers, OSs, and Java virtual machines.

2.1 Source codes

We used the source code (`.java`) in AES CD-2 for each AES candidate. We used the source code in DEAL (`DES_Algorithm.java`) for DES.

All byte codes were generated using the Java compiler, `javac` command in JDK 1.1.7B, with option `-O` for optimization.

2.2 Computer and OS

Abbreviation	NIST
Computer	NIST AES analysis platform
Processor	Pentium Pro 200MHz
Main RAM	64MB
OS	Windows95

Abbreviation	UE450
Computer	Sun Ultra Enterprise 450
Processor	UltraSPARC–II 296MHz (×2)
Main RAM	512MB
OS	SunOS 5.6

Abbreviation	VAIO
Computer	SONY PCG–505EX
Processor	MMX Pentium 233MHz
Main RAM	32MB
OS	Windows95/Linux 2.2.1

2.3 Java virtual machines

We summarize Java virtual machines indicating their distribution points and the results of `java -fullversion` (JDK) or `netscape -java -version` (Navigator) for each virtual machine.

- JDK 1.2

  for Windows JDK 1.2 for Windows
  `http://www.javasoft.com`
  `/products/jdk/1.2/`
  `"JDK-1.2-V"`

- JDK 1.1.7

  for Windows JDK 1.1.7B for Windows
  `http://www.javasoft.com`
  `/products/jdk/1.1/`
  `"JDK1.1.7U"`

  for SunOS 5 JDK 1.1.7 Production Release (3/29/99)
  `http://www.sun.com/solaris/java/`
  `"Solaris_JDK_1.1.7_06"`

  for Linux JDK 1.1.7v1a
  `http://www.blackdown.org`
  `/java-linux.html`
  `"Linux_JDK_1.1.7_v1a_green_threads"`

- Netscape Navigator 4.08 (SunOS 5, Linux)
  `ftp://ftp.netscape.com/pub/communicator`
  `/4.08/english/unix/`
  `-java version 98306`

*Contact person: Kazumaro Aoki (Email: `maro@isl.ntt.co.jp`)

There are two JDKs whose version number is the same for SunOS 5.

- Reference Implementation
- Production Release

The former was developed by Java Software in Sun Microsystems Inc. The latter was optimized from the former by Solaris Software. We used the latter.

JDK for Linux was ported from the code of JDK for SunOS 5 by volunteers.

2.4 Just In Time compiler

We used the following Just In Time compiler (JIT).

Sun JIT JIT developed by Sun Microsystems Inc. and included in JDK for SunOS 5/SPARC,x86.

Symantec JIT JIT developed by Symantec and included in JDK for Windows.

TYA JIT for JDK/Linux,FreeBSD/x86.
`ftp://gonzalez.cyberus.ca/pub/Linux/java/`

shuJIT JIT for JDK/Linux,FreeBSD/x86.
`http://www.shudo.net/jit/index-j.html`

JDK for SunOS 5 and Windows use Sun JIT and Symantec JIT, respectively, unless JIT is specified. Because JDK for Linux does not include JIT, we used the two above JIT packages where noted. There is no JIT which can be used with Navigator for UNIX.

3 How to measure

We measured the following.

- 1 block encryption and decryption (basic API)
- key setup (basic API)
- large block encryption and decryption (extended API)

However, we did not measure the timing for DES needed for extended API, because the NIST implementation for extended API requires that the block size of basic API be 128 bits even though the code of DES requires that the block size be 64 bits.

One block encryption and decryption We used `blockEncrypt()` for encryption and `blockDecrypt()` for decryption in the basic API. We measured processor cycles per block (cycles/block) and throughput (Mbits/sec). We measured the cycles per block based on the time just before the loop starts and the time just after the loop ends, where the loop consists of a basic API call for the same text data and the same key values[1]. We set a number of iterations such that the total process time was at least 1.5 seconds and at most 3.0 seconds on Linux with Pentium 233MHz using JDK 1.1.7 without JIT compiler in the case of the 192-bit key. The number of iterations is multiplied by 10 if the JIT compiler was used.

The results have 3 significant digits because the total process time of each test was more than 1.5 seconds and the resolution of the timer was at most 20 msec.

Key setup We measured cycles per key by calling `makeKey()` in the basic API many times. Method of computing cycles per key is the same as that for measuring one block encryption.

Large block encryption and decryption We measured throughput (Mbits/sec) and cycles per block (cycles/block) using one `doFinal()` call in the extended API.

We computed the cycles per block based on the time just before calling the extended API (`doFinal()`) and the time just after calling the extended API. We set the size of data for ECB and CBC mode such that the total process time was at least 2.5 seconds and at most 5.0 seconds on Linux with Pentium 233MHz using JDK 1.1.7 without JIT compiler in the case of the 256-bit key. We set the size of data for 1-bit CFB at one 128th that of ECB and CBC. We quadrupled the size of data if the JIT compiler was used, but the size was truncated to no less than 1KB and no more than 1MB. The data for encryption and decryption was "000...000".

[1] We used "00010203...0e0f" for the 128-bit key, "00010203...0e0f000102...0607" for the 192-bit key, and "00010203...0e0f000102...0e0f" for the 256-bit key. We used "0123456789abcdef" for DES.

The results have 3 significant digits because the total process time of each test was more than about 2.5 seconds and the resolution of timer was at most 20 msec. Note that the encryption time in a few cases, for example RC6 ECB mode, was quite small, so the significant digits in these cases was about 2.

E2 and RC6 has own implementation of extended API. We measured both own implementation and the implementation included in NIST kit.

4 Description of Results

We summarize the results below:

Computer, OS, Java virtual machine, JIT compiler

We sorted the results for the 128-bit key. Note that the block size of DES is half that of the AES candidates.

The following environments were examined.

- NIST: NIST analysis platform
  - Windows 95
    - JDK 1.2
      - Symantec JIT
      - without JIT
    - JDK 1.1.7
      - Symantec JIT
      - without JIT
- UE450: Sun Ultra Enterprise 450
  - SunOS 5.6
    - JDK 1.1.7
      - Sun JIT
      - without JIT
    - Navigator 4.08
      - without JIT
- VAIO: SONY PCG-505EX
  - Windows95
    - JDK 1.2
      - Symantec JIT
      - without JIT
    - JDK 1.1.7
      - Symantec JIT
      - without JIT
  - Linux
    - JDK 1.1.7
      - without JIT
      - TYA
      - shuJIT
    - Navigator 4.08
      - without JIT

Note that Mbits means 10^6 bits, and Kbits means 10^3 bits in the following tables.

5 Notice

We think that our results have several biases, for example, interrupts, and incompatibility between the source codes and JIT. Thus, the simple ranking of the tables is meaningless. The tables should use for finding tendencies. Especially, we wonder at the difference between JDK1.1.7 and JDK1.2 with Symantec JIT on NIST and VAIO for key setup of Twofish.

6 Results

6.1 One Block Encryption

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1900	1720	1720
Rijndael	2130	2350	2600
E2	2190	2200	2250
MARS	2980	2740	2860
SERPENT	3280	2860	2960
CRYPTON	3290	3190	3240
HPC	3620	3280	3300
DES	2040		
LOKI97	4400	4380	4400
CAST–256	4840	4820	4720
Twofish	5260	5060	5060
SAFER+	8360	10800	14000
FROG	8560	9000	8360
DEAL	20000	19800	26400
MAGENTA	53800	51800	69200
DFC	470000	457000	455000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	13.5	14.9	14.9
Rijndael	12.0	10.9	9.85
E2	11.7	11.6	11.4
MARS	8.59	9.34	8.95
SERPENT	7.80	8.95	8.65
CRYPTON	7.78	8.03	7.90
HPC	7.07	7.80	7.76
DES	6.27		
LOKI97	5.82	5.84	5.82
CAST–256	5.29	5.31	5.42
Twofish	4.87	5.06	5.06
SAFER+	3.06	2.38	1.82
FROG	2.99	2.84	3.06
DEAL	1.28	1.29	0.971
MAGENTA	0.476	0.494	0.370
DFC	0.0545	0.0560	0.0563

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	17500	17600	17500
Rijndael	21200	24500	27500
E2	26900	27500	26900
CRYPTON	37900	37900	37900
HPC	49400	49400	49400
SERPENT	50600	50600	49400
MARS	50600	51600	50400
DES	28000		
CAST–256	61400	63800	62600
Twofish	65800	67000	66000
LOKI97	85600	85800	85600
FROG	123000	121000	123000
SAFER+	141000	209000	274000
DEAL	184000	182000	238000
MAGENTA	682000	692000	900000
DFC	988000	964000	968000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.46	1.45	1.46
Rijndael	1.21	1.04	0.932
E2	0.952	0.931	0.952
CRYPTON	0.675	0.675	0.675
HPC	0.518	0.518	0.518
SERPENT	0.506	0.506	0.518
MARS	0.506	0.496	0.508
DES	0.457		
CAST–256	0.417	0.401	0.409
Twofish	0.389	0.382	0.388
LOKI97	0.299	0.298	0.299
FROG	0.208	0.212	0.208
SAFER+	0.182	0.123	0.0933
DEAL	0.139	0.141	0.108
MAGENTA	0.0375	0.0370	0.0284
DFC	0.0259	0.0266	0.0264

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1910	1910	1870
Rijndael	2270	2530	2820
E2	2310	2310	2260
MARS	3080	2960	3080
SERPENT	3300	2960	2980
CRYPTON	3510	3460	3520
HPC	3840	3640	3620
DES	2140		
LOKI97	4400	4400	4400
CAST–256	5160	5060	5160
Twofish	5280	5040	5160
SAFER+	8320	11000	14300
FROG	8560	8760	8360
DEAL	21800	21800	27500
MAGENTA	57000	55000	73600
DFC	365000	365000	363000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	13.4	13.4	13.7
Rijndael	11.3	10.1	9.08
E2	11.1	11.1	11.3
MARS	8.31	8.65	8.31
SERPENT	7.76	8.65	8.59
CRYPTON	7.29	7.40	7.27
HPC	6.67	7.03	7.07
DES	5.98		
LOKI97	5.82	5.82	5.82
CAST–256	4.96	5.06	4.96
Twofish	4.85	5.08	4.96
SAFER+	3.08	2.34	1.79
FROG	2.99	2.92	3.06
DEAL	1.18	1.18	0.932
MAGENTA	0.449	0.465	0.348
DFC	0.0702	0.0702	0.0706

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	17600	17500	17200
Rijndael	21300	24500	27800
E2	27500	26900	26900
CRYPTON	37900	37900	37900
HPC	50600	49400	50400
SERPENT	50600	50600	50600
MARS	51600	51600	50600
DES	28000		
CAST–256	63800	63600	62600
Twofish	66000	66000	66000
LOKI97	84600	84600	85600
FROG	123000	123000	123000
SAFER+	140000	209000	277000
DEAL	180000	180000	235000
MAGENTA	658000	670000	890000
DFC	788000	788000	792000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.45	1.46	1.49
Rijndael	1.20	1.04	0.921
E2	0.931	0.952	0.952
CRYPTON	0.675	0.675	0.675
HPC	0.506	0.518	0.508
SERPENT	0.506	0.506	0.506
MARS	0.496	0.496	0.506
DES	0.457		
CAST–256	0.401	0.403	0.409
Twofish	0.388	0.388	0.388
LOKI97	0.303	0.303	0.299
FROG	0.208	0.208	0.208
SAFER+	0.182	0.123	0.0925
DEAL	0.142	0.142	0.109
MAGENTA	0.0389	0.0382	0.0288
DFC	0.0325	0.0325	0.0323

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	2940	2940	3020
Rijndael	4110	4440	4910
E2	4550	4370	5070
MARS	5180	5380	5450
HPC	6000	6050	6040
SERPENT	6600	6220	6240
CRYPTON	7050	7520	7860
DES	3650		
Twofish	9770	9800	9910
CAST–256	13000	12300	12300
LOKI97	13200	13400	13600
FROG	20100	20400	20000
SAFER+	26000	38600	50400
DEAL	37200	36500	46400
MAGENTA	111000	112000	151000
DFC	427000	420000	416000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	12.9	12.9	12.6
Rijndael	9.23	8.55	7.74
E2	8.34	8.68	7.49
MARS	7.33	7.06	6.96
HPC	6.32	6.27	6.29
SERPENT	5.75	6.11	6.08
CRYPTON	5.38	5.05	4.83
DES	5.20		
Twofish	3.89	3.87	3.83
CAST–256	2.93	3.08	3.09
LOKI97	2.87	2.82	2.80
FROG	1.89	1.86	1.90
SAFER+	1.46	0.982	0.753
DEAL	1.02	1.04	0.818
MAGENTA	0.341	0.338	0.252
DFC	0.0890	0.0904	0.0913

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	22500	22900	22200
Rijndael	24600	28300	32600
E2	30900	30400	30600
CRYPTON	38600	39200	38100
MARS	48000	48000	48200
HPC	49600	50400	49900
DES	26800		
CAST–256	65200	64000	63700
SERPENT	69200	68400	68800
Twofish	71400	71600	71400
LOKI97	84500	84500	84500
FROG	126000	126000	126000
SAFER+	165000	245000	323000
DEAL	187000	185000	243000
MAGENTA	643000	640000	854000
DFC	796000	767000	762000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.69	1.66	1.71
Rijndael	1.55	1.34	1.17
E2	1.23	1.25	1.24
CRYPTON	0.983	0.969	0.996
MARS	0.791	0.792	0.788
HPC	0.765	0.753	0.761
DES	0.709		
CAST–256	0.582	0.593	0.596
SERPENT	0.549	0.556	0.552
Twofish	0.532	0.530	0.532
LOKI97	0.449	0.449	0.449
FROG	0.302	0.301	0.302
SAFER+	0.230	0.155	0.117
DEAL	0.203	0.205	0.157
MAGENTA	0.0591	0.0594	0.0445
DFC	0.0477	0.0495	0.0498

UE450, SunOS 5.6, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	56100	56300	56200
Rijndael	59900	70100	80000
E2	77700	77700	78100
CRYPTON	94200	94500	94500
HPC	112000	112000	112000
MARS	124000	125000	125000
DES	66300		
CAST–256	161000	161000	163000
Twofish	173000	176000	172000
SERPENT	184000	184000	184000
LOKI97	220000	220000	221000
FROG	345000	344000	343000
SAFER+	384000	575000	764000
DEAL	437000	437000	569000
MAGENTA	1450000	1450000	1940000
DFC	1710000	1680000	1670000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.676	0.675	0.675
Rijndael	0.634	0.542	0.475
E2	0.489	0.489	0.487
CRYPTON	0.403	0.402	0.402
HPC	0.340	0.338	0.339
MARS	0.305	0.304	0.304
DES	0.286		
CAST–256	0.237	0.236	0.233
Twofish	0.220	0.215	0.221
SERPENT	0.207	0.206	0.206
LOKI97	0.173	0.173	0.172
FROG	0.110	0.110	0.111
SAFER+	0.0990	0.0661	0.0497
DEAL	0.0869	0.0868	0.0668
MAGENTA	0.0262	0.0262	0.0196
DFC	0.0222	0.0226	0.0227

VAIO, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
E2	2620	3460	2370
Rijndael	2820	3030	3500
SERPENT	3590	3220	3200
RC6	3590	3550	3460
CRYPTON	4880	4810	4810
MARS	5250	4990	4990
HPC	5510	5390	5370
Twofish	5900	5620	5900
DES	3010		
LOKI97	6930	6930	6930
CAST–256	7440	7300	7190
FROG	11800	11500	11800
SAFER+	14300	18700	24100
DEAL	27900	27700	39000
MAGENTA	69100	66500	89600
DFC	615000	595000	602000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
E2	11.4	8.62	12.6
Rijndael	10.6	9.85	8.53
SERPENT	8.31	9.28	9.34
RC6	8.31	8.42	8.63
CRYPTON	6.12	6.21	6.21
MARS	5.69	5.98	5.98
HPC	5.42	5.54	5.57
Twofish	5.06	5.31	5.06
DES	4.96		
LOKI97	4.31	4.31	4.31
CAST–256	4.01	4.09	4.16
FROG	2.54	2.59	2.53
SAFER+	2.08	1.60	1.24
DEAL	1.07	1.08	0.766
MAGENTA	0.432	0.449	0.333
DFC	0.0486	0.0502	0.0496

VAIO, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16600	16700	16600
Rijndael	19200	21800	25600
E2	23800	25000	24300
CRYPTON	31400	31400	31400
MARS	39700	38500	39700
DES	20500		
HPC	42200	42500	40800
SERPENT	47400	49900	47600
CAST–256	51300	51300	51100
Twofish	61600	64200	62800
LOKI97	70500	71600	70500
FROG	94700	92400	91900
SAFER+	123000	180000	238000
DEAL	149000	149000	192000
MAGENTA	551000	539000	730000
DFC	1030000	999000	999000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.79	1.79	1.79
Rijndael	1.55	1.37	1.17
E2	1.25	1.20	1.23
CRYPTON	0.952	0.952	0.952
MARS	0.753	0.776	0.753
DES	0.727		
HPC	0.707	0.703	0.731
SERPENT	0.631	0.598	0.627
CAST–256	0.582	0.582	0.584
Twofish	0.485	0.465	0.476
LOKI97	0.424	0.417	0.424
FROG	0.315	0.323	0.325
SAFER+	0.242	0.166	0.125
DEAL	0.201	0.201	0.155
MAGENTA	0.0542	0.0554	0.0409
DFC	0.0291	0.0299	0.0299

VAIO, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
Rijndael	2690	3030	3200
RC6	3500	3510	3500
SERPENT	3590	3200	3220
E2	3780	4360	4160
CRYPTON	4810	4860	4810
MARS	5020	4990	4880
HPC	5530	5130	5250
Twofish	5760	5510	5650
DES	3080		
LOKI97	7050	7050	6790
CAST–256	7930	7700	7820
FROG	11800	11500	12100
SAFER+	13900	19000	24400
DEAL	33800	33300	43100
MAGENTA	66700	68100	89600
DFC	528000	518000	510000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
Rijndael	11.1	9.85	9.32
RC6	8.53	8.51	8.53
SERPENT	8.31	9.34	9.28
E2	7.90	6.84	7.17
CRYPTON	6.21	6.14	6.21
MARS	5.95	5.98	6.12
HPC	5.40	5.82	5.69
Twofish	5.18	5.42	5.29
DES	4.85		
LOKI97	4.24	4.24	4.40
CAST–256	3.76	3.88	3.82
FROG	2.53	2.59	2.47
SAFER+	2.15	1.57	1.23
DEAL	0.883	0.896	0.693
MAGENTA	0.448	0.438	0.333
DFC	0.0566	0.0577	0.0586

VAIO, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	17100	17100	16600
Rijndael	18400	20900	24000
E2	25100	24400	25000
CRYPTON	32000	31400	31400
MARS	39700	39700	41100
DES	21100		
HPC	42200	41100	42200
SERPENT	48800	48800	48500
CAST–256	49900	49900	49900
Twofish	60400	61400	61600
LOKI97	69300	70500	70500
FROG	92400	91900	94700
SAFER+	118000	180000	241000
DEAL	154000	148000	190000
MAGENTA	511000	539000	693000
DFC	896000	901000	896000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.75	1.75	1.79
Rijndael	1.63	1.43	1.25
E2	1.19	1.22	1.20
CRYPTON	0.934	0.952	0.952
MARS	0.753	0.753	0.727
DES	0.707		
HPC	0.707	0.727	0.707
SERPENT	0.612	0.612	0.615
CAST–256	0.598	0.598	0.598
Twofish	0.494	0.487	0.485
LOKI97	0.431	0.424	0.424
FROG	0.323	0.325	0.315
SAFER+	0.254	0.166	0.124
DEAL	0.194	0.201	0.157
MAGENTA	0.0584	0.0554	0.0431
DFC	0.0333	0.0332	0.0333

VAIO, Linux, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	15100	15100	15100
Rijndael	16700	19100	22000
E2	21400	21900	21500
CRYPTON	27900	27900	28000
MARS	34400	35200	35500
HPC	36500	37300	37400
DES	19300		
SERPENT	42300	41800	43200
CAST–256	45200	46000	46600
Twofish	55000	55000	55800
LOKI97	62700	63000	63300
FROG	85600	86100	87400
SAFER+	108000	160000	214000
DEAL	134000	133000	172000
MAGENTA	472000	481000	640000
DFC	856000	857000	830000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.98	1.98	1.98
Rijndael	1.79	1.56	1.36
E2	1.40	1.36	1.39
CRYPTON	1.07	1.07	1.07
MARS	0.868	0.848	0.842
HPC	0.818	0.801	0.800
DES	0.774		
SERPENT	0.705	0.714	0.691
CAST–256	0.660	0.649	0.641
Twofish	0.543	0.543	0.535
LOKI97	0.476	0.474	0.472
FROG	0.349	0.347	0.342
SAFER+	0.276	0.186	0.139
DEAL	0.222	0.225	0.173
MAGENTA	0.0632	0.0621	0.0466
DFC	0.0349	0.0348	0.0360

VAIO, Linux, JDK 1.1.7, TYA

Number of cycles (cycles/block)

Key length (bit)	128	192	256
Rijndael	5890	6610	7340
RC6	6190	6170	6150
E2	7030	8180	7090
MARS	9500	10400	10600
DES	6300		
CRYPTON	13100	13000	13000
CAST–256	17700	18900	19200
HPC	18000	18800	18700
Twofish	26700	27300	28200
SERPENT	29900	29400	30300
FROG	32900	32900	34200
LOKI97	36100	35500	36400
SAFER+	53600	77600	103000
DEAL	56400	54900	71000
MAGENTA	169000	177000	234000
DFC	717000	713000	703000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
Rijndael	5.07	4.52	4.07
RC6	4.82	4.84	4.85
E2	4.25	3.65	4.21
MARS	3.14	2.88	2.81
DES	2.37		
CRYPTON	2.29	2.30	2.30
CAST–256	1.68	1.58	1.56
HPC	1.66	1.59	1.60
Twofish	1.12	1.09	1.06
SERPENT	1.00	1.01	0.986
FROG	0.907	0.907	0.874
LOKI97	0.827	0.841	0.821
SAFER+	0.557	0.385	0.290
DEAL	0.530	0.544	0.420
MAGENTA	0.177	0.169	0.127
DFC	0.0417	0.0419	0.0425

VAIO, Linux, JDK 1.1.7, shuJIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
Rijndael	5420	6040	6640
E2	6380	7500	7070
RC6	6490	6420	6390
MARS	8280	9080	9430
DES	6220		
HPC	13900	14600	14500
CRYPTON	16600	16200	16300
LOKI97	25100	24900	25600
FROG	27700	27900	29000
CAST–256	27800	28500	28700
SERPENT	32600	32100	33100
Twofish	55300	55900	55300
DEAL	60100	59900	74400
SAFER+	103000	147000	193000
MAGENTA	160000	168000	222000
DFC	974000	968000	951000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
Rijndael	5.51	4.95	4.50
E2	4.68	3.98	4.22
RC6	4.60	4.65	4.67
MARS	3.61	3.29	3.17
DES	2.40		
HPC	2.15	2.04	2.06
CRYPTON	1.80	1.84	1.83
LOKI97	1.19	1.20	1.17
FROG	1.08	1.07	1.03
CAST–256	1.08	1.05	1.04
SERPENT	0.916	0.932	0.903
Twofish	0.540	0.534	0.540
DEAL	0.497	0.499	0.402
SAFER+	0.290	0.203	0.155
MAGENTA	0.187	0.178	0.134
DFC	0.0307	0.0308	0.0314

VAIO, Linux, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	45200	45600	45500
Rijndael	50700	59200	67700
E2	64300	64800	64900
CRYPTON	81000	81900	81700
MARS	99600	100000	100000
HPC	104000	105000	104000
DES	54900		
CAST–256	140000	141000	140000
SERPENT	146000	147000	146000
Twofish	149000	149000	149000
LOKI97	216000	215000	216000
FROG	241000	241000	241000
SAFER+	314000	469000	621000
DEAL	365000	368000	477000
MAGENTA	1240000	1250000	1660000
DFC	1580000	1540000	1550000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.661	0.654	0.656
Rijndael	0.590	0.505	0.441
E2	0.465	0.461	0.460
CRYPTON	0.369	0.365	0.366
MARS	0.300	0.297	0.299
HPC	0.288	0.285	0.287
DES	0.272		
CAST–256	0.214	0.212	0.213
SERPENT	0.205	0.204	0.205
Twofish	0.200	0.200	0.200
LOKI97	0.139	0.139	0.138
FROG	0.124	0.124	0.124
SAFER+	0.0950	0.0637	0.0481
DEAL	0.0818	0.0811	0.0626
MAGENTA	0.0241	0.0239	0.0180
DFC	0.0189	0.0193	0.0193

6.2 One Block Decryption

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1830	1760	1790
Rijndael	2120	2310	2630
E2	2200	2250	2300
MARS	2960	2740	2860
CRYPTON	3290	3180	3190
SERPENT	3400	2960	2960
HPC	3740	3520	3620
DES	2030		
LOKI97	4500	4280	4280
CAST–256	4820	4820	4740
Twofish	5160	5040	5060
FROG	5920	5920	5960
SAFER+	8560	11400	14700
DEAL	20000	19800	26400
MAGENTA	52600	52800	69200
DFC	461000	455000	464000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	14.0	14.5	14.3
Rijndael	12.1	11.1	9.72
E2	11.6	11.4	11.1
MARS	8.65	9.34	8.95
CRYPTON	7.78	8.05	8.03
SERPENT	7.53	8.65	8.65
HPC	6.84	7.27	7.07
DES	6.31		
LOKI97	5.69	5.98	5.98
CAST–256	5.31	5.31	5.40
Twofish	4.96	5.08	5.06
FROG	4.32	4.32	4.30
SAFER+	2.99	2.25	1.74
DEAL	1.28	1.30	0.971
MAGENTA	0.487	0.485	0.370
DFC	0.0555	0.0563	0.0552

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	18300	18300	17900
Rijndael	21200	24200	27500
E2	26900	26300	26400
CRYPTON	37900	37900	37900
HPC	50600	51600	50600
SERPENT	52800	53800	51600
MARS	53800	53800	52800
DES	27500		
CAST–256	62600	62800	62600
Twofish	67000	67000	65800
LOKI97	86800	85600	85800
FROG	105000	106000	106000
SAFER+	141000	209000	272000
DEAL	185000	182000	237000
MAGENTA	680000	682000	902000
DFC	944000	988000	968000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.40	1.40	1.43
Rijndael	1.21	1.06	0.932
E2	0.952	0.973	0.970
CRYPTON	0.675	0.675	0.675
HPC	0.506	0.496	0.506
SERPENT	0.485	0.476	0.496
MARS	0.476	0.476	0.485
DES	0.465		
CAST–256	0.409	0.408	0.409
Twofish	0.382	0.382	0.389
LOKI97	0.295	0.299	0.298
FROG	0.243	0.242	0.242
SAFER+	0.182	0.123	0.0940
DEAL	0.139	0.140	0.108
MAGENTA	0.0376	0.0375	0.0284
DFC	0.0271	0.0259	0.0264

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1830	1800	1790
Rijndael	2310	2490	2740
E2	2360	2250	2310
MARS	3080	2960	2960
SERPENT	3400	3200	3060
CRYPTON	3510	3460	3510
HPC	3860	3740	3840
DES	2140		
LOKI97	4400	4280	4380
CAST–256	5160	5040	5160
Twofish	5260	5160	5040
FROG	6160	5960	5720
SAFER+	8800	11600	15000
DEAL	21800	21300	27000
MAGENTA	56000	55000	73600
DFC	347000	356000	354000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	14.0	14.2	14.3
Rijndael	11.1	10.3	9.34
E2	10.8	11.4	11.1
MARS	8.31	8.65	8.65
SERPENT	7.53	8.00	8.37
CRYPTON	7.29	7.40	7.29
HPC	6.63	6.84	6.67
DES	5.98		
LOKI97	5.82	5.98	5.84
CAST–256	4.96	5.08	4.96
Twofish	4.87	4.96	5.08
FROG	4.16	4.30	4.48
SAFER+	2.91	2.20	1.71
DEAL	1.18	1.20	0.948
MAGENTA	0.457	0.465	0.348
DFC	0.0737	0.0719	0.0724

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	17600	17900	17200
Rijndael	21600	24500	28200
E2	26300	27000	26300
CRYPTON	37900	37900	37900
HPC	50600	50600	50600
MARS	52600	53800	53800
SERPENT	52800	51600	51600
DES	30200		
CAST–256	62600	63600	63800
Twofish	66000	65800	67000
LOKI97	84600	85800	85600
FROG	110000	108000	108000
SAFER+	141000	209000	279000
DEAL	180000	180000	235000
MAGENTA	660000	670000	878000
DFC	788000	772000	792000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.45	1.43	1.49
Rijndael	1.19	1.04	0.908
E2	0.973	0.948	0.973
CRYPTON	0.675	0.675	0.675
HPC	0.506	0.506	0.506
MARS	0.487	0.476	0.476
SERPENT	0.485	0.496	0.496
DES	0.424		
CAST–256	0.409	0.403	0.401
Twofish	0.388	0.389	0.382
LOKI97	0.303	0.298	0.299
FROG	0.233	0.238	0.238
SAFER+	0.182	0.123	0.0918
DEAL	0.142	0.142	0.109
MAGENTA	0.0388	0.0382	0.0292
DFC	0.0325	0.0332	0.0323

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	2960	2980	2970
Rijndael	4080	4220	4730
E2	4140	4460	4430
MARS	5250	5410	5550
HPC	6210	6390	6720
SERPENT	6750	6430	6450
CRYPTON	6990	7880	8020
DES	3660		
Twofish	9740	9810	9880
CAST–256	13000	12300	12200
LOKI97	13200	13300	13600
FROG	20000	20500	20100
SAFER+	25100	37200	48600
DEAL	37100	36300	46100
MAGENTA	112000	113000	151000
DFC	410000	414000	418000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	12.8	12.7	12.8
Rijndael	9.32	9.01	8.02
E2	9.18	8.51	8.58
MARS	7.23	7.02	6.84
HPC	6.12	5.95	5.65
SERPENT	5.63	5.91	5.89
CRYPTON	5.43	4.82	4.74
DES	5.19		
Twofish	3.90	3.87	3.84
CAST–256	2.92	3.08	3.12
LOKI97	2.88	2.85	2.79
FROG	1.90	1.85	1.89
SAFER+	1.51	1.02	0.782
DEAL	1.02	1.05	0.823
MAGENTA	0.339	0.335	0.252
DFC	0.0927	0.0917	0.0909

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	22500	23300	22500
Rijndael	26400	30600	35100
E2	30300	30700	30600
CRYPTON	39000	39300	38500
MARS	49500	49800	49600
HPC	51400	51500	51500
DES	26800		
CAST–256	64900	63900	63500
SERPENT	68900	68400	68900
Twofish	71300	71800	71700
LOKI97	84300	84800	84600
FROG	120000	119000	122000
SAFER+	165000	244000	324000
DEAL	186000	185000	242000
MAGENTA	640000	638000	853000
DFC	769000	761000	767000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.69	1.63	1.69
Rijndael	1.44	1.24	1.08
E2	1.25	1.24	1.24
CRYPTON	0.973	0.966	0.985
MARS	0.768	0.763	0.766
HPC	0.739	0.737	0.737
DES	0.710		
CAST–256	0.585	0.594	0.598
SERPENT	0.551	0.555	0.551
Twofish	0.533	0.529	0.530
LOKI97	0.451	0.448	0.449
FROG	0.317	0.320	0.312
SAFER+	0.230	0.156	0.117
DEAL	0.204	0.206	0.157
MAGENTA	0.0593	0.0596	0.0445
DFC	0.0494	0.0499	0.0495

6.3 Key Setup

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	318	406	496
DES	3180		
CRYPTON	10200	10100	10100
RC6	12300	12100	12300
MARS	15000	14700	14600
LOKI97	16500	15400	15900
SAFER+	19200	28600	41700
Rijndael	23700	27000	30600
E2	25300	24200	24100
SERPENT	41800	38400	37200
DEAL	52700	51100	65900
CAST–256	79100	78600	79100
Twofish	85800	90000	95600
HPC	136000	134000	136000
DFC	1860000	1830000	1830000
FROG	5280000	4940000	4940000

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	3180	4300	5480
CRYPTON	43000	42800	42800
DES	41200		
Rijndael	92000	104000	123000
RC6	108000	105000	108000
E2	209000	216000	220000
SAFER+	220000	395000	637000
MARS	245000	249000	245000
LOKI97	269000	264000	258000
CAST–256	396000	395000	395000
DEAL	494000	494000	638000
Twofish	714000	934000	1130000
SERPENT	802000	768000	780000
HPC	1520000	1520000	1540000
DFC	3890000	3900000	3960000
FROG	86800000	85800000	85600000

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	406	494	584
DES	3030		
CRYPTON	9000	9020	9120
RC6	11400	11400	11200
MARS	12900	12100	12100
LOKI97	14900	13700	13800
SAFER+	17000	25900	38500
Rijndael	22000	24400	27500
E2	24500	23800	24100
SERPENT	37400	35200	36200
Twofish	48400	52800	59400
DEAL	51600	50600	65300
CAST–256	79100	78600	79600
HPC	123000	121000	121000
DFC	1430000	1420000	1430000
FROG	4720000	4500000	4500000

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	3300	4280	5600
CRYPTON	40600	41600	43000
Rijndael	90000	101000	123000
DES	45100		
RC6	106000	110000	108000
E2	205000	213000	223000
SAFER+	214000	401000	648000
MARS	249000	241000	245000
LOKI97	269000	258000	259000
CAST–256	384000	385000	390000
DEAL	488000	489000	631000
Twofish	682000	890000	1080000
SERPENT	780000	770000	780000
HPC	1490000	1500000	1500000
DFC	3180000	3190000	3240000
FROG	86600000	85600000	85800000

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	1120	1430	1660
DES	4460		
CRYPTON	11400	11300	11400
RC6	17500	17900	18000
MARS	29500	30500	30700
Rijndael	36100	41700	47300
SAFER+	38500	69700	112000
LOKI97	40700	39500	39300
E2	44400	44600	46300
SERPENT	64300	63600	63700
DEAL	80100	78300	102000
CAST–256	110000	111000	113000
Twofish	122000	152000	182000
HPC	129000	128000	131000
DFC	1690000	1690000	1710000
FROG	10200000	10000000	10100000

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	4700	6410	8280
CRYPTON	41500	43200	44900
DES	37400		
Rijndael	96200	107000	133000
RC6	105000	108000	109000
E2	206000	221000	225000
MARS	222000	225000	224000
LOKI97	253000	250000	247000
SAFER+	263000	490000	794000
CAST–256	381000	393000	396000
DEAL	479000	464000	616000
Twofish	668000	868000	1090000
SERPENT	1060000	1050000	1060000
HPC	1510000	1530000	1530000
DFC	3210000	3180000	3200000
FROG	102000000	102000000	101000000

UE450, SunOS 5.6, Navigator 4.08, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	10800	15000	19500
CRYPTON	94300	97800	101000
Rijndael	189000	218000	265000
DES	95500		
RC6	259000	262000	265000
E2	517000	546000	569000
MARS	537000	540000	546000
SAFER+	596000	1150000	1900000
LOKI97	652000	643000	636000
CAST–256	893000	901000	909000
DEAL	1130000	1140000	1480000
Twofish	1660000	2290000	2920000
SERPENT	2720000	2720000	2710000
HPC	3640000	3640000	3640000
DFC	6860000	6820000	6890000
FROG	245000000	244000000	244000000

VAIO, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	539	667	807
DES	5120		
CRYPTON	17400	17400	17600
RC6	22100	21300	21800
MARS	23900	23000	23100
LOKI97	25500	25000	25000
SAFER+	30100	43600	62800
Rijndael	34300	39500	44800
E2	35500	33800	36300
DEAL	78200	75000	96100
SERPENT	93600	88400	89600
CAST–256	127000	125000	124000
Twofish	147000	156000	165000
HPC	190000	187000	187000
DFC	2400000	2350000	2350000
FROG	7930000	7160000	7300000

VAIO, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	742	873	975
DES	4680		
CRYPTON	16500	16100	16100
RC6	20800	20500	21000
MARS	20900	20100	20500
LOKI97	23700	23000	22500
SAFER+	26900	40400	57600
Rijndael	35400	41500	46900
E2	46600	43900	43600
Twofish	75600	83300	92200
DEAL	79400	76900	101000
SERPENT	85900	84500	84700
CAST–256	129000	129000	130000
HPC	167000	167000	169000
DFC	2070000	2060000	2080000
FROG	7050000	6530000	6670000

VAIO, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	2940	3970	5250
CRYPTON	42200	41100	43400
DES	32000		
Rijndael	89600	105000	123000
RC6	94700	92400	97500
E2	180000	184000	188000
MARS	192000	187000	188000
SAFER+	212000	371000	590000
LOKI97	218000	224000	218000
CAST–256	345000	346000	352000
DEAL	398000	391000	506000
Twofish	616000	782000	924000
SERPENT	793000	744000	744000
HPC	1280000	1260000	1260000
DFC	4040000	3980000	4040000
FROG	77000000	75600000	74400000

VAIO, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	3220	4080	5390
CRYPTON	39700	41100	40800
DES	30800		
Rijndael	92400	108000	128000
RC6	95200	91900	91900
E2	184000	193000	201000
MARS	184000	184000	184000
SAFER+	205000	372000	602000
LOKI97	218000	211000	205000
CAST–256	359000	352000	352000
DEAL	397000	391000	513000
Twofish	551000	705000	870000
SERPENT	756000	756000	744000
HPC	1230000	1200000	1260000
DFC	3390000	3520000	3590000
FROG	74200000	74200000	74200000

VAIO, Linux, JDK 1.1.7, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	2860	3840	4940
CRYPTON	34600	35200	36700
DES	28200		
RC6	80700	82400	83400
Rijndael	81800	92800	114000
E2	159000	168000	174000
MARS	167000	168000	169000
SAFER+	174000	322000	523000
LOKI97	192000	188000	186000
CAST–256	311000	314000	316000
DEAL	354000	350000	462000
Twofish	491000	636000	773000
SERPENT	677000	676000	678000
HPC	1080000	1090000	1090000
DFC	3450000	3420000	3440000
FROG	68000000	67600000	67300000

VAIO, Linux, JDK 1.1.7, shuJIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	1440	1840	2320
DES	8280		
RC6	31200	32200	32500
Rijndael	46600	53800	66500
MARS	48800	49600	50000
SAFER+	59700	103000	162000
CRYPTON	60100	60600	60500
E2	68200	71100	74400
LOKI97	79200	75800	74900
DEAL	137000	129000	174000
SERPENT	174000	172000	172000
Twofish	185000	221000	261000
CAST–256	203000	203000	204000
HPC	272000	272000	273000
DFC	3850000	3790000	3790000
FROG	19900000	19600000	19400000

VAIO, Linux, JDK 1.1.7, TYA

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	1240	1750	2270
DES	9290		
RC6	32200	33700	33900
CRYPTON	32400	33000	32800
Rijndael	47400	54600	68200
MARS	53800	55100	55600
SAFER+	62900	107000	171000
E2	68400	72100	72300
LOKI97	110000	108000	107000
DEAL	137000	129000	174000
CAST–256	175000	173000	173000
SERPENT	205000	200000	200000
Twofish	207000	250000	295000
HPC	423000	425000	426000
DFC	2830000	2780000	2780000
FROG	22500000	22300000	21900000

VAIO, Linux, Navigator 4.08, w/o JIT

Number of cycles (cycles/key)

Key length (bit)	128	192	256
MAGENTA	9310	12700	16500
CRYPTON	84100	86800	89500
DES	77600		
Rijndael	172000	198000	239000
RC6	213000	218000	220000
E2	426000	450000	470000
MARS	440000	444000	448000
SAFER+	481000	913000	1480000
LOKI97	645000	640000	633000
CAST–256	807000	818000	825000
DEAL	942000	950000	1230000
Twofish	1430000	1890000	2360000
SERPENT	2140000	2150000	2140000
HPC	3430000	3450000	3460000
DFC	6300000	6280000	6300000
FROG	201000000	200000000	199000000

6.4 Large Blocks Encryption

E2 and RC6 have their own extended API implementation. We measured the timing of both, their implementation, and the implementation included in the NIST kit for E2 and RC6. In the tables, "Algorithm name" means the timing derived using own implementation, and "Algorithm name-NIST" means the timing derived using NIST kit implementation.

6.4.1 ECB mode

We summarize the number of cycles (cycles/block) and throughput (Mbits/sec) below.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	854	1010	1010
E2	2200	2170	2010
RC6-NIST	6040	6010	6200
Rijndael	6680	7020	7390
E2-NIST	6710	6870	6710
MARS	7540	7230	7200
SERPENT	8060	8030	7870
CRYPTON	8060	8060	8210
HPC	8390	8390	8540
LOKI97	9030	9090	9340
Twofish	9890	9890	10000
CAST–256	10100	10100	9890
FROG	12800	12800	12700
SAFER+	12800	16100	19400
DEAL	26100	26100	32800
MAGENTA	61500	62000	80600
DFC	504000	488000	523000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	30.0	25.4	25.4
E2	11.7	11.8	12.7
RC6-NIST	4.24	4.26	4.13
Rijndael	3.83	3.65	3.47
E2-NIST	3.81	3.73	3.81
MARS	3.40	3.54	3.55
SERPENT	3.18	3.19	3.25
CRYPTON	3.18	3.18	3.12
HPC	3.05	3.05	3.00
LOKI97	2.83	2.81	2.74
Twofish	2.59	2.59	2.55
CAST–256	2.54	2.54	2.59
FROG	2.01	2.01	2.02
SAFER+	2.00	1.59	1.32
DEAL	0.980	0.980	0.780
MAGENTA	0.416	0.413	0.318
DFC	0.0508	0.0525	0.0490

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	15800	15900	15800
E2	27800	27800	28100
RC6-NIST	28500	28800	29000
Rijndael	32200	35900	39600
E2-NIST	38900	38900	39200
CRYPTON	49700	50300	49600
SERPENT	61000	62300	61800
HPC	61800	61600	61600
MARS	62300	62400	61800
CAST–256	73700	74500	73700
Twofish	77800	77800	77800
LOKI97	97900	96700	97700
FROG	131000	133000	131000
SAFER+	150000	220000	287000
DEAL	196000	196000	250000
MAGENTA	687000	697000	922000
DFC	955000	934000	998000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.62	1.61	1.62
E2	0.920	0.920	0.910
RC6-NIST	0.899	0.888	0.883
Rijndael	0.796	0.713	0.647
E2-NIST	0.658	0.657	0.653
CRYPTON	0.515	0.509	0.517
SERPENT	0.419	0.411	0.414
HPC	0.414	0.415	0.415
MARS	0.411	0.410	0.414
CAST–256	0.347	0.344	0.347
Twofish	0.329	0.329	0.329
LOKI97	0.261	0.265	0.262
FROG	0.195	0.193	0.195
SAFER+	0.170	0.116	0.0893
DEAL	0.131	0.131	0.103
MAGENTA	0.0372	0.0367	0.0278
DFC	0.0268	0.0274	0.0257

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	824	824	824
E2	2350	2350	2320
RC6-NIST	5370	5370	5370
E2-NIST	5550	5520	5370
Rijndael	5710	5890	6350
MARS	6200	6380	6350
SERPENT	6530	6560	6680
HPC	7050	7020	7050
CRYPTON	7390	7690	7390
LOKI97	8360	8360	8360
Twofish	8540	8700	8390
CAST–256	9220	9400	9400
FROG	12100	12100	12100
SAFER+	12800	16100	18700
DEAL	30900	30900	38200
MAGENTA	58600	59100	80600
DFC	352000	335000	365000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	31.1	31.1	31.1
E2	10.9	10.9	11.0
RC6-NIST	4.77	4.77	4.77
E2-NIST	4.61	4.63	4.77
Rijndael	4.49	4.35	4.03
MARS	4.13	4.01	4.03
SERPENT	3.92	3.90	3.83
HPC	3.63	3.65	3.63
CRYPTON	3.47	3.33	3.47
LOKI97	3.06	3.06	3.06
Twofish	3.00	2.94	3.05
CAST–256	2.78	2.72	2.72
FROG	2.12	2.12	2.12
SAFER+	2.00	1.59	1.37
DEAL	0.829	0.829	0.670
MAGENTA	0.437	0.433	0.318
DFC	0.0728	0.0763	0.0702

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	15900	16100	15900
RC6-NIST	26500	26800	26600
E2	27200	27200	27500
Rijndael	30900	34200	37500
E2-NIST	36200	36600	36500
CRYPTON	48300	48200	48200
HPC	59100	59700	60300
SERPENT	60300	60400	60300
MARS	60900	61000	61000
CAST–256	73100	73700	73700
Twofish	75700	75800	75800
LOKI97	95200	97900	95200
FROG	133000	133000	132000
SAFER+	153000	217000	287000
DEAL	193000	193000	247000
MAGENTA	666000	664000	902000
DFC	762000	752000	781000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.61	1.59	1.61
RC6-NIST	0.966	0.954	0.961
E2	0.943	0.943	0.932
Rijndael	0.829	0.749	0.682
E2-NIST	0.707	0.700	0.701
CRYPTON	0.530	0.531	0.531
HPC	0.433	0.429	0.425
SERPENT	0.425	0.424	0.425
MARS	0.420	0.419	0.419
CAST–256	0.350	0.347	0.347
Twofish	0.338	0.338	0.338
LOKI97	0.269	0.261	0.269
FROG	0.193	0.193	0.195
SAFER+	0.168	0.118	0.0892
DEAL	0.133	0.132	0.104
MAGENTA	0.0384	0.0386	0.0284
DFC	0.0336	0.0340	0.0328

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1740	1780	1750
E2	4280	4220	4160
RC6-NIST	7860	7920	7890
Rijndael	9400	10200	10500
E2-NIST	10700	10400	10400
MARS	10800	10600	10600
HPC	11600	11400	11300
SERPENT	12200	12200	12200
CRYPTON	12700	12800	12700
Twofish	14800	14700	14800
CAST–256	18400	17300	17300
LOKI97	19200	19300	19100
FROG	25100	25500	25500
SAFER+	32100	43000	56400
DEAL	42100	42500	52800
MAGENTA	118000	117000	153000
DFC	416000	398000	429000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	21.8	21.3	21.7
E2	8.87	8.99	9.14
RC6-NIST	4.83	4.79	4.81
Rijndael	4.04	3.74	3.60
E2-NIST	3.54	3.65	3.66
MARS	3.51	3.57	3.59
HPC	3.28	3.34	3.35
SERPENT	3.11	3.11	3.11
CRYPTON	2.98	2.97	3.00
Twofish	2.57	2.58	2.56
CAST–256	2.06	2.19	2.19
LOKI97	1.98	1.97	1.98
FROG	1.52	1.49	1.49
SAFER+	1.18	0.883	0.673
DEAL	0.902	0.894	0.719
MAGENTA	0.323	0.324	0.248
DFC	0.0913	0.0953	0.0886

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	24700	24800	24800
E2	33000	32900	32200
RC6-NIST	33700	33700	33800
Rijndael	36300	40300	43800
E2-NIST	42900	42900	42700
CRYPTON	50500	50800	50000
MARS	59800	58700	59600
HPC	61700	61000	61800
CAST–256	79700	77900	78700
SERPENT	80400	81600	80200
Twofish	84300	83200	82600
LOKI97	96800	96900	96900
FROG	138000	137000	137000
SAFER+	176000	258000	339000
DEAL	208000	207000	265000
MAGENTA	643000	640000	853000
DFC	796000	760000	796000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.54	1.53	1.53
E2	1.15	1.15	1.18
RC6-NIST	1.13	1.13	1.12
Rijndael	1.05	0.942	0.867
E2-NIST	0.886	0.885	0.890
CRYPTON	0.752	0.747	0.760
MARS	0.635	0.647	0.638
HPC	0.615	0.622	0.614
CAST–256	0.476	0.487	0.482
SERPENT	0.472	0.465	0.474
Twofish	0.451	0.456	0.459
LOKI97	0.392	0.392	0.392
FROG	0.275	0.278	0.278
SAFER+	0.216	0.147	0.112
DEAL	0.183	0.184	0.143
MAGENTA	0.0590	0.0593	0.0445
DFC	0.0477	0.0500	0.0477

UE450, SunOS 5.6, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	59300	59800	59400
E2	78400	77900	79200
RC6-NIST	80000	80200	80000
Rijndael	85200	96000	106000
E2-NIST	103000	103000	103000
CRYPTON	120000	121000	120000
HPC	137000	137000	137000
MARS	145000	145000	145000
CAST–256	191000	186000	187000
Twofish	193000	194000	193000
SERPENT	210000	210000	210000
LOKI97	243000	244000	243000
FROG	330000	328000	328000
SAFER+	412000	604000	791000
DEAL	459000	461000	592000
MAGENTA	1480000	1480000	1970000
DFC	1690000	1640000	1710000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.640	0.635	0.639
E2	0.484	0.488	0.479
RC6-NIST	0.475	0.474	0.474
Rijndael	0.445	0.396	0.359
E2-NIST	0.369	0.370	0.369
CRYPTON	0.316	0.315	0.316
HPC	0.277	0.277	0.278
MARS	0.262	0.262	0.262
CAST–256	0.198	0.204	0.203
Twofish	0.197	0.195	0.196
SERPENT	0.181	0.181	0.181
LOKI97	0.156	0.156	0.156
FROG	0.115	0.116	0.116
SAFER+	0.0922	0.0628	0.0480
DEAL	0.0827	0.0824	0.0641
MAGENTA	0.0257	0.0256	0.0192
DFC	0.0225	0.0231	0.0222

VAIO, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1960	1740	1960
E2	3920	4090	3920
RC6-NIST	8220	9010	8790
Rijndael	8580	9010	9190
MARS	9360	9760	9220
E2-NIST	10200	10400	10400
HPC	10400	10400	10100
Twofish	11000	11000	10900
CRYPTON	11500	10800	11500
CAST–256	13300	13100	13300
LOKI97	13300	14500	13000
SERPENT	13700	13300	13500
FROG	17200	17200	17200
SAFER+	19700	25100	30500
DEAL	39000	39200	44600
MAGENTA	68900	71800	97400
DFC	623000	601000	670000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	15.3	17.1	15.3
E2	7.63	7.29	7.63
RC6-NIST	3.63	3.32	3.40
Rijndael	3.48	3.32	3.25
MARS	3.19	3.06	3.24
E2-NIST	2.93	2.88	2.88
HPC	2.88	2.88	2.94
Twofish	2.72	2.72	2.73
CRYPTON	2.59	2.77	2.59
CAST–256	2.24	2.28	2.24
LOKI97	2.24	2.07	2.30
SERPENT	2.18	2.25	2.21
FROG	1.73	1.73	1.73
SAFER+	1.52	1.19	0.980
DEAL	0.765	0.763	0.670
MAGENTA	0.433	0.416	0.307
DFC	0.0480	0.0497	0.0446

VAIO, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	14800	14900	14800
E2	26200	25800	25400
RC6-NIST	27600	27200	27200
Rijndael	29800	32500	35600
E2-NIST	37500	38000	38000
CRYPTON	43000	43000	43000
MARS	50000	50800	50000
HPC	54000	54800	55500
SERPENT	61800	61800	63400
CAST–256	64200	64900	63400
Twofish	74300	74200	74300
LOKI97	84300	82900	86000
FROG	107000	107000	106000
SAFER+	132000	194000	250000
DEAL	163000	166000	216000
MAGENTA	588000	563000	738000
DFC	1050000	1030000	1080000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	2.01	2.01	2.01
E2	1.14	1.16	1.17
RC6-NIST	1.08	1.10	1.10
Rijndael	1.00	0.920	0.839
E2-NIST	0.796	0.787	0.787
CRYPTON	0.694	0.694	0.694
MARS	0.597	0.587	0.597
HPC	0.553	0.545	0.538
SERPENT	0.483	0.483	0.471
CAST–256	0.465	0.460	0.471
Twofish	0.402	0.403	0.402
LOKI97	0.354	0.360	0.347
FROG	0.280	0.280	0.281
SAFER+	0.227	0.154	0.119
DEAL	0.183	0.180	0.138
MAGENTA	0.0508	0.0531	0.0405
DFC	0.0284	0.0291	0.0278

VAIO, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1960	1920	1960
E2	4310	4310	4490
Rijndael	6840	7010	7050
RC6-NIST	7620	7830	7620
CRYPTON	9190	8830	8790
MARS	9190	9190	9010
Twofish	9400	9610	9580
E2-NIST	9580	9010	8790
HPC	10200	9970	10200
SERPENT	10600	10600	10500
LOKI97	12100	12200	11700
CAST–256	12700	13100	12300
FROG	16400	16400	16000
SAFER+	19700	25100	30500
DEAL	43700	43000	52400
MAGENTA	75200	75200	100000
DFC	566000	545000	582000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	15.3	15.5	15.3
E2	6.93	6.93	6.66
Rijndael	4.37	4.26	4.24
RC6-NIST	3.92	3.81	3.92
CRYPTON	3.25	3.38	3.40
MARS	3.25	3.25	3.32
Twofish	3.18	3.11	3.12
E2-NIST	3.12	3.32	3.40
HPC	2.93	3.00	2.93
SERPENT	2.82	2.82	2.83
LOKI97	2.47	2.45	2.56
CAST–256	2.35	2.28	2.42
FROG	1.82	1.82	1.86
SAFER+	1.52	1.19	0.980
DEAL	0.683	0.694	0.570
MAGENTA	0.397	0.397	0.298
DFC	0.0527	0.0548	0.0514

VAIO, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	14800	15100	14700
E2	25400	25100	25800
RC6-NIST	25400	25800	25400
Rijndael	28200	31600	34500
E2-NIST	35600	35600	35600
CRYPTON	42300	42300	42200
MARS	50000	50100	49300
HPC	53300	52400	52400
SERPENT	59500	59500	60200
CAST–256	63400	61800	62500
Twofish	71900	72100	71900
LOKI97	84300	82900	81500
FROG	103000	105000	103000
SAFER+	134000	191000	251000
DEAL	162000	166000	210000
MAGENTA	538000	551000	713000
DFC	852000	825000	864000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	2.01	1.98	2.04
E2	1.17	1.19	1.16
RC6-NIST	1.17	1.16	1.17
Rijndael	1.06	0.945	0.867
E2-NIST	0.839	0.839	0.839
CRYPTON	0.706	0.706	0.708
MARS	0.597	0.596	0.606
HPC	0.561	0.570	0.570
SERPENT	0.502	0.502	0.496
CAST–256	0.471	0.483	0.478
Twofish	0.415	0.414	0.415
LOKI97	0.354	0.360	0.367
FROG	0.289	0.285	0.289
SAFER+	0.222	0.157	0.119
DEAL	0.184	0.180	0.142
MAGENTA	0.0555	0.0542	0.0419
DFC	0.0350	0.0362	0.0346

VAIO, Linux, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	13600	13500	13500
E2	22500	23000	22900
RC6-NIST	23100	23100	23300
Rijndael	25400	28000	30600
E2-NIST	30600	30200	30400
CRYPTON	37400	37400	37600
MARS	44300	44400	44200
HPC	46800	47000	46800
SERPENT	53100	53000	52900
CAST–256	57600	57700	57700
Twofish	64800	64600	64400
LOKI97	73700	71900	73000
FROG	94700	95700	95300
SAFER+	117000	170000	222000
DEAL	145000	146000	187000
MAGENTA	486000	486000	656000
DFC	879000	839000	881000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	2.20	2.21	2.21
E2	1.33	1.30	1.30
RC6-NIST	1.29	1.29	1.28
Rijndael	1.18	1.06	0.975
E2-NIST	0.977	0.987	0.981
CRYPTON	0.798	0.799	0.794
MARS	0.675	0.673	0.675
HPC	0.638	0.635	0.638
SERPENT	0.563	0.563	0.565
CAST–256	0.519	0.517	0.517
Twofish	0.461	0.462	0.464
LOKI97	0.405	0.415	0.409
FROG	0.315	0.312	0.313
SAFER+	0.255	0.176	0.135
DEAL	0.205	0.204	0.160
MAGENTA	0.0614	0.0614	0.0455
DFC	0.0340	0.0356	0.0339

VAIO, Linux, JDK 1.1.7, TYA

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	4480	4480	4480
E2	9320	9210	9260
RC6-NIST	11000	10900	10900
Rijndael	11900	12500	13600
E2-NIST	15100	15100	15200
MARS	16500	16400	16400
CRYPTON	23200	22600	22700
HPC	26300	26400	26200
CAST–256	27800	27600	27600
Twofish	35100	34900	35000
SERPENT	38200	38300	38200
FROG	39500	39600	38700
LOKI97	42900	42400	42500
SAFER+	65200	89100	113000
DEAL	66100	68400	83300
MAGENTA	180000	180000	235000
DFC	685000	674000	708000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	6.66	6.67	6.67
E2	3.20	3.24	3.23
RC6-NIST	2.73	2.73	2.73
Rijndael	2.52	2.39	2.20
E2-NIST	1.97	1.98	1.97
MARS	1.81	1.82	1.82
CRYPTON	1.29	1.32	1.32
HPC	1.14	1.13	1.14
CAST–256	1.07	1.08	1.08
Twofish	0.851	0.856	0.854
SERPENT	0.781	0.780	0.783
FROG	0.757	0.754	0.772
LOKI97	0.697	0.705	0.703
SAFER+	0.458	0.335	0.263
DEAL	0.452	0.437	0.358
MAGENTA	0.166	0.166	0.127
DFC	0.0436	0.0443	0.0422

VAIO, Linux, JDK 1.1.7, shuJIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	4440	4410	4410
E2	8500	8420	8570
RC6-NIST	14200	14500	14100
Rijndael	14200	14800	15500
E2-NIST	16100	15900	16100
MARS	17600	17600	17600
HPC	24700	24700	24500
CRYPTON	30200	30000	30100
FROG	34900	35100	34200
LOKI97	38100	37400	37400
CAST–256	40500	40000	40100
SERPENT	49500	49600	49600
Twofish	60300	59900	60000
DEAL	73800	74000	93800
SAFER+	115000	158000	203000
MAGENTA	172000	173000	226000
DFC	921000	902000	940000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	6.73	6.77	6.77
E2	3.51	3.55	3.48
RC6-NIST	2.10	2.06	2.11
Rijndael	2.10	2.02	1.92
E2-NIST	1.85	1.88	1.86
MARS	1.70	1.70	1.70
HPC	1.21	1.21	1.22
CRYPTON	0.989	0.996	0.992
FROG	0.857	0.852	0.874
LOKI97	0.783	0.798	0.799
CAST–256	0.737	0.746	0.744
SERPENT	0.603	0.602	0.602
Twofish	0.496	0.499	0.498
DEAL	0.405	0.404	0.319
SAFER+	0.260	0.189	0.147
MAGENTA	0.173	0.173	0.132
DFC	0.0324	0.0331	0.0318

VAIO, Linux, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	42400	42300	42300
E2	65700	65300	65500
RC6-NIST	68200	67900	68200
Rijndael	73800	82400	90700
E2-NIST	88900	88300	88600
CRYPTON	106000	106000	105000
MARS	123000	123000	123000
HPC	128000	128000	128000
CAST–256	164000	165000	164000
SERPENT	170000	171000	170000
Twofish	173000	173000	173000
LOKI97	240000	240000	239000
FROG	265000	265000	264000
SAFER+	336000	492000	644000
DEAL	392000	394000	503000
MAGENTA	1270000	1270000	1680000
DFC	1550000	1520000	1560000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.704	0.707	0.707
E2	0.455	0.457	0.456
RC6-NIST	0.438	0.440	0.438
Rijndael	0.405	0.363	0.329
E2-NIST	0.336	0.338	0.337
CRYPTON	0.283	0.283	0.285
MARS	0.243	0.243	0.243
HPC	0.233	0.233	0.233
CAST–256	0.182	0.181	0.182
SERPENT	0.175	0.175	0.175
Twofish	0.173	0.173	0.173
LOKI97	0.124	0.124	0.125
FROG	0.113	0.113	0.113
SAFER+	0.0889	0.0607	0.0464
DEAL	0.0762	0.0759	0.0593
MAGENTA	0.0235	0.0235	0.0178
DFC	0.0192	0.0197	0.0191

6.4.2 CBC mode

We summarize the number of cycles (cycles/block) and throughput (Mbits/sec) below.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	977	1010	1010
E2	3510	3360	3510
RC6-NIST	8060	8210	8210
E2-NIST	8880	8880	8880
Rijndael	8880	9250	9550
SERPENT	9550	9580	9700
MARS	9890	9890	9890
HPC	10400	10400	10600
CRYPTON	10600	10600	10600
LOKI97	11100	11400	11400
Twofish	11700	11900	11700
CAST–256	12200	12200	12400
FROG	15100	15100	14800
SAFER+	15400	18200	22100
DEAL	28200	28100	36900
MAGENTA	64000	64500	83000
DFC	539000	528000	534000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	26.2	25.4	25.4
E2	7.29	7.63	7.29
RC6-NIST	3.18	3.12	3.12
E2-NIST	2.88	2.88	2.88
Rijndael	2.88	2.77	2.68
SERPENT	2.68	2.67	2.64
MARS	2.59	2.59	2.59
HPC	2.46	2.46	2.42
CRYPTON	2.42	2.42	2.42
LOKI97	2.30	2.26	2.24
Twofish	2.18	2.15	2.18
CAST–256	2.09	2.09	2.06
FROG	1.70	1.69	1.73
SAFER+	1.66	1.41	1.16
DEAL	0.908	0.912	0.694
MAGENTA	0.400	0.397	0.308
DFC	0.0475	0.0485	0.0480

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16400	16600	16400
E2	32200	32500	32500
RC6-NIST	33500	33500	33500
Rijndael	37900	41600	44900
E2-NIST	43900	44300	43900
CRYPTON	54900	55100	54900
SERPENT	66400	66400	66400
HPC	67000	66400	66400
MARS	67000	67000	67000
CAST–256	78500	79700	79800
Twofish	83100	83100	83100
LOKI97	103000	103000	103000
FROG	137000	137000	138000
SAFER+	158000	225000	292000
DEAL	199000	201000	257000
MAGENTA	697000	697000	922000
DFC	1010000	986000	977000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.56	1.54	1.56
E2	0.796	0.787	0.787
RC6-NIST	0.763	0.764	0.763
Rijndael	0.675	0.616	0.570
E2-NIST	0.583	0.579	0.583
CRYPTON	0.466	0.465	0.466
SERPENT	0.386	0.386	0.386
HPC	0.382	0.386	0.386
MARS	0.382	0.382	0.382
CAST–256	0.326	0.321	0.321
Twofish	0.308	0.308	0.308
LOKI97	0.248	0.248	0.248
FROG	0.187	0.187	0.185
SAFER+	0.162	0.114	0.0875
DEAL	0.129	0.127	0.0995
MAGENTA	0.0367	0.0367	0.0278
DFC	0.0254	0.0260	0.0262

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1010	1010	1010
E2	3510	3540	3510
RC6-NIST	7200	7200	7200
E2-NIST	7390	7390	7390
Rijndael	7900	8390	8700
MARS	8730	8700	8910
SERPENT	8880	8700	8880
HPC	9060	9060	9060
CRYPTON	9890	9700	9890
Twofish	10400	10600	10600
LOKI97	10700	10700	10400
CAST–256	11400	11200	11400
FROG	14400	14400	14400
SAFER+	15400	18200	22100
DEAL	32200	32800	40300
MAGENTA	61500	64500	80600
DFC	378000	365000	365000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	25.4	25.4	25.4
E2	7.29	7.23	7.29
RC6-NIST	3.55	3.55	3.55
E2-NIST	3.47	3.47	3.47
Rijndael	3.24	3.05	2.94
MARS	2.93	2.94	2.87
SERPENT	2.88	2.94	2.88
HPC	2.82	2.82	2.82
CRYPTON	2.59	2.64	2.59
Twofish	2.46	2.42	2.42
LOKI97	2.38	2.38	2.47
CAST–256	2.25	2.28	2.25
FROG	1.78	1.78	1.78
SAFER+	1.66	1.41	1.16
DEAL	0.794	0.780	0.636
MAGENTA	0.416	0.397	0.318
DFC	0.0677	0.0702	0.0702

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16600	16600	16600
RC6-NIST	31200	31500	31300
E2	32200	31900	31900
Rijndael	35900	39200	42600
E2-NIST	41600	41600	41200
CRYPTON	53600	54300	53600
SERPENT	64900	66400	65700
HPC	65800	64900	65100
MARS	66400	66400	66300
CAST–256	78500	78500	78400
Twofish	79800	79800	79800
LOKI97	101000	101000	101000
FROG	137000	138000	139000
SAFER+	156000	223000	292000
DEAL	196000	196000	250000
MAGENTA	676000	676000	900000
DFC	805000	783000	795000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.54	1.54	1.54
RC6-NIST	0.821	0.813	0.817
E2	0.796	0.804	0.804
Rijndael	0.713	0.653	0.601
E2-NIST	0.616	0.615	0.621
CRYPTON	0.478	0.471	0.478
SERPENT	0.394	0.386	0.390
HPC	0.389	0.394	0.393
MARS	0.386	0.386	0.386
CAST–256	0.326	0.326	0.327
Twofish	0.321	0.321	0.321
LOKI97	0.255	0.255	0.255
FROG	0.187	0.185	0.184
SAFER+	0.164	0.115	0.0877
DEAL	0.131	0.131	0.103
MAGENTA	0.0379	0.0379	0.0284
DFC	0.0318	0.0327	0.0322

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1780	1800	1800
E2	6200	6070	6110
RC6-NIST	10600	10600	10600
Rijndael	12300	12600	13300
MARS	13100	13100	12900
E2-NIST	13500	13500	13500
HPC	14400	14300	14300
CRYPTON	15200	15400	15400
SERPENT	16000	15900	15900
Twofish	18000	17900	17800
CAST–256	20200	20400	20400
LOKI97	25300	25100	24600
FROG	28900	27900	28000
SAFER+	34700	47200	62700
DEAL	45500	45800	54800
MAGENTA	121000	121000	161000
DFC	443000	433000	435000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	21.3	21.1	21.1
E2	6.12	6.26	6.22
RC6-NIST	3.59	3.57	3.57
Rijndael	3.08	3.03	2.86
MARS	2.91	2.91	2.94
E2-NIST	2.80	2.80	2.81
HPC	2.64	2.66	2.66
CRYPTON	2.49	2.47	2.47
SERPENT	2.37	2.39	2.39
Twofish	2.12	2.12	2.13
CAST–256	1.88	1.86	1.86
LOKI97	1.50	1.51	1.54
FROG	1.31	1.36	1.36
SAFER+	1.10	0.804	0.606
DEAL	0.834	0.828	0.693
MAGENTA	0.315	0.315	0.236
DFC	0.0857	0.0876	0.0874

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	25600	25600	25600
E2	37100	36800	36900
RC6-NIST	40200	40300	40300
Rijndael	42300	46600	50900
E2-NIST	49600	49500	49300
CRYPTON	56700	56900	56300
MARS	65500	65700	65700
HPC	67700	67500	67500
CAST–256	81700	82800	81800
SERPENT	87300	86300	87500
Twofish	91000	91000	90800
LOKI97	102000	104000	102000
FROG	143000	145000	143000
SAFER+	184000	267000	348000
DEAL	215000	212000	274000
MAGENTA	650000	652000	881000
DFC	817000	809000	783000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.49	1.49	1.48
E2	1.02	1.03	1.03
RC6-NIST	0.945	0.942	0.941
Rijndael	0.897	0.815	0.746
E2-NIST	0.765	0.768	0.770
CRYPTON	0.670	0.668	0.674
MARS	0.580	0.578	0.578
HPC	0.561	0.563	0.562
CAST–256	0.465	0.458	0.464
SERPENT	0.435	0.440	0.434
Twofish	0.418	0.417	0.418
LOKI97	0.373	0.365	0.371
FROG	0.266	0.262	0.266
SAFER+	0.206	0.142	0.109
DEAL	0.177	0.179	0.138
MAGENTA	0.0584	0.0582	0.0431
DFC	0.0465	0.0469	0.0485

UE450, SunOS 5.6, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	64300	64200	64100
E2	88500	88800	88300
RC6-NIST	92700	92300	92500
Rijndael	98600	109000	119000
E2-NIST	115000	115000	115000
CRYPTON	133000	132000	132000
HPC	149000	149000	149000
MARS	157000	156000	157000
CAST–256	198000	198000	199000
Twofish	206000	206000	206000
SERPENT	222000	222000	221000
LOKI97	257000	256000	256000
FROG	341000	341000	342000
SAFER+	420000	608000	792000
DEAL	477000	478000	609000
MAGENTA	1500000	1490000	1980000
DFC	1750000	1710000	1710000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.591	0.591	0.592
E2	0.429	0.428	0.430
RC6-NIST	0.410	0.411	0.410
Rijndael	0.385	0.349	0.318
E2-NIST	0.330	0.330	0.330
CRYPTON	0.286	0.287	0.287
HPC	0.254	0.254	0.255
MARS	0.242	0.243	0.242
CAST–256	0.192	0.192	0.191
Twofish	0.184	0.184	0.184
SERPENT	0.171	0.171	0.172
LOKI97	0.148	0.148	0.148
FROG	0.111	0.111	0.111
SAFER+	0.0905	0.0625	0.0479
DEAL	0.0796	0.0794	0.0624
MAGENTA	0.0254	0.0254	0.0192
DFC	0.0217	0.0222	0.0222

VAIO, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1960	1920	1960
E2	8580	8790	8620
Rijndael	10500	11700	12300
RC6-NIST	11100	11100	11100
MARS	13100	14100	13500
CRYPTON	13300	13500	13300
E2-NIST	13900	14300	14500
HPC	14100	14300	14100
Twofish	14300	14100	14100
CAST–256	16200	16400	16400
SERPENT	16600	16800	16800
LOKI97	18000	17600	17200
FROG	19900	20400	20300
SAFER+	24400	29800	36000
DEAL	42200	41400	47700
MAGENTA	75200	75200	104000
DFC	644000	653000	660000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	15.3	15.5	15.3
E2	3.48	3.40	3.47
Rijndael	2.83	2.54	2.42
RC6-NIST	2.68	2.68	2.68
MARS	2.28	2.12	2.21
CRYPTON	2.24	2.21	2.25
E2-NIST	2.15	2.09	2.07
HPC	2.12	2.09	2.12
Twofish	2.09	2.12	2.12
CAST–256	1.84	1.82	1.82
SERPENT	1.80	1.77	1.77
LOKI97	1.66	1.70	1.74
FROG	1.50	1.47	1.47
SAFER+	1.23	1.00	0.829
DEAL	0.708	0.721	0.626
MAGENTA	0.397	0.397	0.288
DFC	0.0464	0.0457	0.0452

VAIO, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	15200	15500	15200
E2	31700	32500	32000
RC6-NIST	33300	33600	34000
Rijndael	36300	39900	42200
E2-NIST	44200	43400	43400
CRYPTON	50100	48600	48400
MARS	56400	56300	56300
HPC	61100	61000	61800
SERPENT	69600	68800	68800
CAST–256	70400	71200	71200
Twofish	80600	80600	81300
LOKI97	90600	94000	92300
FROG	113000	113000	114000
SAFER+	144000	197000	260000
DEAL	169000	169000	216000
MAGENTA	565000	574000	752000
DFC	1100000	1090000	1100000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.96	1.93	1.96
E2	0.943	0.920	0.932
RC6-NIST	0.898	0.888	0.877
Rijndael	0.822	0.748	0.707
E2-NIST	0.675	0.688	0.689
CRYPTON	0.596	0.615	0.617
MARS	0.530	0.531	0.531
HPC	0.489	0.490	0.483
SERPENT	0.429	0.434	0.434
CAST–256	0.425	0.419	0.419
Twofish	0.371	0.371	0.367
LOKI97	0.330	0.318	0.324
FROG	0.265	0.265	0.261
SAFER+	0.207	0.152	0.115
DEAL	0.177	0.177	0.138
MAGENTA	0.0529	0.0520	0.0397
DFC	0.0271	0.0274	0.0271

VAIO, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1960	1920	1960
E2	9190	9010	9190
Rijndael	10400	11200	11500
RC6-NIST	10500	10400	10600
E2-NIST	11500	12500	12700
MARS	11700	11900	11700
CRYPTON	12100	12500	12500
Twofish	12500	12500	12700
HPC	12700	13100	13100
SERPENT	12900	12700	12900
LOKI97	16000	16000	16800
CAST–256	16200	16000	15600
FROG	19600	19900	19600
SAFER+	22600	28200	34500
DEAL	47000	46100	57100
MAGENTA	78600	78600	103000
DFC	579000	573000	575000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	15.3	15.5	15.3
E2	3.25	3.32	3.25
Rijndael	2.88	2.67	2.59
RC6-NIST	2.83	2.88	2.82
E2-NIST	2.59	2.39	2.35
MARS	2.54	2.50	2.54
CRYPTON	2.46	2.38	2.39
Twofish	2.38	2.38	2.35
HPC	2.35	2.28	2.28
SERPENT	2.31	2.35	2.31
LOKI97	1.86	1.86	1.78
CAST–256	1.84	1.86	1.91
FROG	1.53	1.50	1.53
SAFER+	1.32	1.06	0.867
DEAL	0.636	0.647	0.523
MAGENTA	0.380	0.380	0.290
DFC	0.0516	0.0521	0.0519

VAIO, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	15500	15200	15300
RC6-NIST	31100	31500	30900
E2	32000	31600	31700
Rijndael	34000	37200	39900
E2-NIST	40700	40300	40200
CRYPTON	50100	50800	49300
MARS	57100	56300	56400
HPC	58700	57800	59500
SERPENT	66500	66400	68100
CAST–256	69600	69600	68800
Twofish	77500	78900	77500
LOKI97	87400	89200	89200
FROG	108000	110000	109000
SAFER+	134000	197000	260000
DEAL	166000	172000	212000
MAGENTA	538000	551000	713000
DFC	900000	877000	864000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.93	1.96	1.96
RC6-NIST	0.961	0.948	0.966
E2	0.932	0.945	0.943
Rijndael	0.877	0.804	0.749
E2-NIST	0.735	0.741	0.742
CRYPTON	0.596	0.587	0.606
MARS	0.523	0.531	0.530
HPC	0.509	0.517	0.502
SERPENT	0.449	0.450	0.439
CAST–256	0.429	0.429	0.434
Twofish	0.386	0.379	0.386
LOKI97	0.342	0.335	0.335
FROG	0.277	0.272	0.273
SAFER+	0.222	0.152	0.115
DEAL	0.180	0.174	0.141
MAGENTA	0.0555	0.0542	0.0419
DFC	0.0332	0.0340	0.0346

VAIO, Linux, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	14000	14000	14000
RC6-NIST	27600	27600	27600
E2	28200	27900	27800
Rijndael	30100	32500	35400
E2-NIST	36100	35900	35600
CRYPTON	43700	43500	43400
MARS	50100	49900	49900
HPC	52600	52700	52000
SERPENT	58600	58300	58400
CAST–256	62600	62800	62200
Twofish	69600	69600	69500
LOKI97	78200	78200	78400
FROG	99700	99400	99800
SAFER+	122000	175000	227000
DEAL	151000	151000	192000
MAGENTA	494000	492000	651000
DFC	884000	880000	869000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	2.13	2.14	2.14
RC6-NIST	1.08	1.08	1.08
E2	1.06	1.07	1.08
Rijndael	0.992	0.918	0.843
E2-NIST	0.827	0.833	0.839
CRYPTON	0.684	0.687	0.688
MARS	0.597	0.599	0.599
HPC	0.568	0.567	0.575
SERPENT	0.509	0.512	0.512
CAST–256	0.477	0.475	0.480
Twofish	0.429	0.429	0.430
LOKI97	0.382	0.382	0.381
FROG	0.300	0.300	0.299
SAFER+	0.245	0.171	0.131
DEAL	0.198	0.198	0.156
MAGENTA	0.0605	0.0607	0.0459
DFC	0.0338	0.0339	0.0344

VAIO, Linux, JDK 1.1.7, TYA

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	4610	4610	4600
E2	13200	13000	13000
RC6-NIST	15500	15400	15600
Rijndael	16100	16900	17900
E2-NIST	18800	19300	18800
MARS	21700	21600	21900
CRYPTON	26900	26700	26800
HPC	30600	30400	30500
CAST–256	33100	32800	32700
Twofish	39200	39200	39200
FROG	44100	43800	43900
SERPENT	45600	45500	45500
LOKI97	47200	47000	47900
SAFER+	69000	96000	117000
DEAL	73800	74300	89900
MAGENTA	185000	185000	242000
DFC	747000	731000	730000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	6.47	6.48	6.49
E2	2.26	2.30	2.30
RC6-NIST	1.92	1.93	1.91
Rijndael	1.86	1.76	1.67
E2-NIST	1.59	1.55	1.59
MARS	1.37	1.38	1.36
CRYPTON	1.11	1.12	1.11
HPC	0.975	0.983	0.980
CAST–256	0.903	0.910	0.914
Twofish	0.761	0.761	0.761
FROG	0.677	0.682	0.681
SERPENT	0.655	0.656	0.656
LOKI97	0.633	0.635	0.623
SAFER+	0.433	0.311	0.255
DEAL	0.405	0.402	0.332
MAGENTA	0.161	0.162	0.124
DFC	0.0400	0.0409	0.0409

VAIO, Linux, JDK 1.1.7, shuJIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	4540	4540	4550
E2	12800	12700	12700
RC6-NIST	17100	17500	17200
Rijndael	19300	20000	20800
E2-NIST	21900	21700	21500
MARS	21900	21600	21600
HPC	29400	28800	28800
CRYPTON	35500	35600	35400
LOKI97	40500	40600	40500
FROG	40700	40200	39600
CAST–256	46200	46300	46400
SERPENT	49900	49500	49500
Twofish	67500	67300	67500
DEAL	78600	78700	95200
SAFER+	118000	168000	210000
MAGENTA	176000	176000	229000
DFC	1010000	987000	988000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	6.58	6.58	6.57
E2	2.34	2.36	2.36
RC6-NIST	1.75	1.71	1.73
Rijndael	1.55	1.49	1.44
E2-NIST	1.37	1.37	1.39
MARS	1.37	1.38	1.38
HPC	1.02	1.04	1.04
CRYPTON	0.842	0.840	0.845
LOKI97	0.737	0.736	0.737
FROG	0.734	0.743	0.755
CAST–256	0.646	0.644	0.644
SERPENT	0.599	0.603	0.603
Twofish	0.442	0.444	0.443
DEAL	0.380	0.379	0.314
SAFER+	0.253	0.178	0.142
MAGENTA	0.170	0.170	0.130
DFC	0.0295	0.0302	0.0302

VAIO, Linux, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	43700	43800	43700
E2	76400	76600	76300
RC6-NIST	79500	79500	79500
Rijndael	85700	94000	102000
E2-NIST	99900	100000	99700
CRYPTON	116000	117000	116000
MARS	134000	134000	135000
HPC	140000	140000	140000
CAST–256	177000	177000	176000
SERPENT	183000	183000	183000
Twofish	184000	185000	184000
LOKI97	252000	252000	251000
FROG	277000	277000	277000
SAFER+	349000	503000	652000
DEAL	407000	405000	515000
MAGENTA	1280000	1280000	1700000
DFC	1630000	1590000	1590000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	0.683	0.682	0.684
E2	0.391	0.390	0.391
RC6-NIST	0.376	0.376	0.376
Rijndael	0.348	0.318	0.292
E2-NIST	0.299	0.298	0.300
CRYPTON	0.257	0.256	0.257
MARS	0.222	0.222	0.222
HPC	0.213	0.213	0.213
CAST–256	0.169	0.169	0.169
SERPENT	0.163	0.163	0.163
Twofish	0.162	0.162	0.162
LOKI97	0.119	0.118	0.119
FROG	0.108	0.108	0.108
SAFER+	0.0857	0.0594	0.0458
DEAL	0.0735	0.0738	0.0580
MAGENTA	0.0233	0.0233	0.0176
DFC	0.0183	0.0187	0.0188

6.4.3 1-bit CFB mode

We summarize the number of cycles (cycles/block) and throughput (Kbits/sec) below. Note that the unit of throughput differs from that for the ECB and CBC modes.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	95700	91800	96700
E2	396000	408000	408000
RC6-NIST	724000	724000	725000
Rijndael	848000	891000	922000
MARS	898000	902000	879000
SERPENT	902000	898000	898000
E2-NIST	955000	955000	953000
CRYPTON	965000	965000	969000
HPC	1010000	1010000	1030000
LOKI97	1110000	1120000	1120000
Twofish	1180000	1200000	1180000
CAST–256	1270000	1250000	1270000
FROG	1590000	1590000	1590000
SAFER+	1720000	2140000	2580000
DEAL	3520000	3590000	4380000
MAGENTA	7380000	7530000	9440000
DFC	60800000	60400000	60300000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	267	279	265
E2	64.6	62.7	62.7
RC6-NIST	35.4	35.4	35.3
Rijndael	30.2	28.7	27.8
MARS	28.5	28.4	29.1
SERPENT	28.4	28.5	28.5
E2-NIST	26.8	26.8	26.9
CRYPTON	26.5	26.5	26.4
HPC	25.4	25.4	24.8
LOKI97	23.1	22.9	22.9
Twofish	21.7	21.3	21.7
CAST–256	20.2	20.5	20.2
FROG	16.1	16.1	16.1
SAFER+	14.9	12.0	9.93
DEAL	7.28	7.12	5.85
MAGENTA	3.47	3.40	2.71
DFC	0.421	0.424	0.425

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1850000	1870000	1870000
RC6-NIST	3480000	3450000	3460000
Rijndael	3950000	4420000	4800000
E2	4210000	4250000	4200000
E2-NIST	4840000	4840000	4890000
CRYPTON	6090000	6190000	6170000
HPC	7640000	7640000	7640000
SERPENT	7640000	7720000	7640000
MARS	7720000	7720000	7730000
CAST–256	9530000	9520000	9450000
Twofish	9700000	9780000	9690000
LOKI97	12200000	12400000	12200000
FROG	16600000	16700000	16800000
SAFER+	19100000	28000000	36400000
DEAL	25000000	24700000	31800000
MAGENTA	87700000	87900000	116000000
DFC	125000000	124000000	124000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.9	13.7	13.7
RC6-NIST	7.36	7.41	7.41
Rijndael	6.48	5.79	5.33
E2	6.08	6.02	6.09
E2-NIST	5.29	5.29	5.23
CRYPTON	4.20	4.14	4.15
HPC	3.35	3.35	3.35
SERPENT	3.35	3.32	3.35
MARS	3.32	3.32	3.31
CAST–256	2.69	2.69	2.71
Twofish	2.64	2.62	2.64
LOKI97	2.10	2.07	2.10
FROG	1.54	1.54	1.52
SAFER+	1.34	0.915	0.703
DEAL	1.02	1.04	0.806
MAGENTA	0.292	0.291	0.220
DFC	0.205	0.206	0.206

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	90800	90800	96700
E2	439000	439000	449000
RC6-NIST	622000	628000	622000
Rijndael	676000	707000	740000
MARS	750000	750000	773000
E2-NIST	805000	805000	805000
SERPENT	816000	836000	816000
HPC	879000	883000	879000
CRYPTON	902000	902000	879000
LOKI97	992000	945000	945000
Twofish	1030000	1050000	1030000
CAST–256	1140000	1160000	1140000
FROG	1450000	1460000	1500000
SAFER+	1530000	2060000	2480000
DEAL	3420000	3440000	4130000
MAGENTA	7530000	7560000	9630000
DFC	46300000	46300000	46300000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	282	282	265
E2	58.3	58.3	57.0
RC6-NIST	41.2	40.8	41.2
Rijndael	37.9	36.2	34.6
MARS	34.1	34.1	33.1
E2-NIST	31.8	31.8	31.8
SERPENT	31.4	30.6	31.4
HPC	29.1	29.0	29.1
CRYPTON	28.4	28.4	29.1
LOKI97	25.8	27.1	27.1
Twofish	24.8	24.4	24.9
CAST–256	22.5	22.1	22.5
FROG	17.6	17.5	17.1
SAFER+	16.7	12.4	10.3
DEAL	7.48	7.45	6.21
MAGENTA	3.40	3.39	2.66
DFC	0.552	0.552	0.552

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1890000	1890000	1890000
RC6-NIST	3260000	3290000	3280000
Rijndael	3730000	4200000	4680000
E2	4200000	4210000	4200000
E2-NIST	4720000	4720000	4770000
CRYPTON	5840000	5920000	5920000
HPC	7450000	7470000	7470000
SERPENT	7470000	7550000	7550000
MARS	7640000	7720000	7640000
CAST–256	9280000	9270000	9360000
Twofish	9440000	9440000	9440000
LOKI97	12000000	12200000	12000000
FROG	16800000	16800000	16800000
SAFER+	19100000	28000000	36600000
DEAL	24400000	24200000	31300000
MAGENTA	85500000	85500000	114000000
DFC	99200000	99100000	99200000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.6	13.6	13.6
RC6-NIST	7.85	7.79	7.80
Rijndael	6.86	6.09	5.47
E2	6.09	6.08	6.09
E2-NIST	5.43	5.43	5.37
CRYPTON	4.38	4.32	4.32
HPC	3.43	3.43	3.43
SERPENT	3.43	3.39	3.39
MARS	3.35	3.32	3.35
CAST–256	2.76	2.76	2.74
Twofish	2.71	2.71	2.71
LOKI97	2.13	2.10	2.13
FROG	1.52	1.52	1.52
SAFER+	1.34	0.915	0.700
DEAL	1.05	1.06	0.819
MAGENTA	0.300	0.299	0.225
DFC	0.258	0.258	0.258

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	184000	184000	184000
E2	734000	738000	749000
RC6-NIST	982000	980000	973000
Rijndael	1120000	1200000	1270000
MARS	1270000	1240000	1260000
E2-NIST	1370000	1340000	1360000
SERPENT	1520000	1520000	1520000
HPC	1520000	1480000	1510000
CRYPTON	1540000	1550000	1600000
Twofish	2070000	1920000	2050000
CAST–256	2190000	2230000	2220000
LOKI97	2440000	2430000	2450000
FROG	3180000	3410000	3170000
SAFER+	4130000	5550000	7220000
DEAL	5370000	5520000	6580000
MAGENTA	15200000	15200000	19900000
DFC	54700000	54900000	54900000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	207	207	207
E2	51.7	51.4	50.7
RC6-NIST	38.7	38.7	39.0
Rijndael	33.9	31.6	29.9
MARS	29.9	30.7	30.1
E2-NIST	27.7	28.3	28.0
SERPENT	25.1	25.0	25.0
HPC	25.0	25.7	25.1
CRYPTON	24.7	24.5	23.7
Twofish	18.3	19.8	18.6
CAST–256	17.3	17.1	17.1
LOKI97	15.6	15.6	15.5
FROG	11.9	11.1	12.0
SAFER+	9.19	6.84	5.26
DEAL	7.08	6.88	5.77
MAGENTA	2.49	2.50	1.91
DFC	0.694	0.692	0.692

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	2870000	2850000	2840000
RC6-NIST	4330000	4310000	4330000
Rijndael	4490000	5010000	5550000
E2	4850000	4850000	4860000
E2-NIST	5470000	5510000	5470000
CRYPTON	6910000	6890000	6860000
HPC	7870000	7730000	7840000
MARS	7950000	7800000	7880000
CAST–256	10300000	10100000	10300000
SERPENT	10300000	10400000	10400000
Twofish	10500000	10800000	10500000
LOKI97	12400000	12400000	12400000
FROG	17400000	17400000	17500000
SAFER+	22700000	33000000	43500000
DEAL	25300000	25300000	32500000
MAGENTA	82200000	82300000	109000000
DFC	101000000	101000000	101000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.2	13.3	13.4
RC6-NIST	8.77	8.81	8.78
Rijndael	8.46	7.57	6.84
E2	7.84	7.83	7.81
E2-NIST	6.94	6.89	6.95
CRYPTON	5.50	5.51	5.54
HPC	4.82	4.91	4.84
MARS	4.78	4.87	4.82
CAST–256	3.70	3.75	3.70
SERPENT	3.69	3.64	3.66
Twofish	3.61	3.52	3.61
LOKI97	3.07	3.07	3.06
FROG	2.18	2.18	2.17
SAFER+	1.67	1.15	0.872
DEAL	1.50	1.50	1.17
MAGENTA	0.462	0.461	0.349
DFC	0.376	0.376	0.376

UE450, SunOS 5.6, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	6830000	6820000	6830000
RC6-NIST	10200000	10200000	10200000
Rijndael	10700000	12000000	13300000
E2	11700000	11700000	11700000
E2-NIST	13000000	13100000	13000000
CRYPTON	15100000	15200000	15100000
HPC	17800000	17800000	17800000
MARS	19200000	19100000	19300000
CAST–256	24100000	24000000	23900000
Twofish	24600000	24800000	24700000
SERPENT	26700000	27100000	27000000
LOKI97	31200000	31300000	31100000
FROG	42100000	41700000	42000000
SAFER+	52400000	76700000	101000000
DEAL	58800000	58900000	75800000
MAGENTA	191000000	191000000	253000000
DFC	218000000	218000000	218000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	5.56	5.57	5.56
RC6-NIST	3.73	3.74	3.74
Rijndael	3.54	3.16	2.85
E2	3.25	3.24	3.24
E2-NIST	2.91	2.91	2.91
CRYPTON	2.51	2.50	2.52
HPC	2.14	2.13	2.14
MARS	1.98	1.98	1.97
CAST–256	1.58	1.58	1.59
Twofish	1.54	1.53	1.54
SERPENT	1.42	1.40	1.41
LOKI97	1.22	1.21	1.22
FROG	0.901	0.910	0.905
SAFER+	0.724	0.495	0.375
DEAL	0.646	0.645	0.501
MAGENTA	0.199	0.199	0.150
DFC	0.174	0.174	0.175

VAIO, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	201000	201000	201000
E2	927000	937000	925000
Rijndael	1040000	1110000	1110000
RC6-NIST	1110000	1110000	1090000
MARS	1280000	1230000	1250000
CRYPTON	1380000	1350000	1400000
Twofish	1380000	1350000	1380000
HPC	1380000	1380000	1380000
SERPENT	1580000	1580000	1580000
LOKI97	1600000	1660000	1600000
CAST–256	1780000	1730000	1700000
E2-NIST	1870000	1880000	1880000
FROG	2110000	2200000	2210000
SAFER+	2810000	3500000	4210000
DEAL	4590000	4610000	5710000
MAGENTA	9410000	9630000	12600000
DFC	88900000	88300000	88300000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	149	149	149
E2	32.2	31.9	32.3
Rijndael	28.7	26.8	26.8
RC6-NIST	26.8	27.0	27.3
MARS	23.4	24.4	23.8
CRYPTON	21.7	22.1	21.3
Twofish	21.7	22.1	21.7
HPC	21.7	21.6	21.7
SERPENT	18.9	18.9	18.9
LOKI97	18.6	18.0	18.7
CAST–256	16.8	17.3	17.5
E2-NIST	16.0	15.9	15.9
FROG	14.2	13.6	13.5
SAFER+	10.6	8.53	7.09
DEAL	6.50	6.48	5.23
MAGENTA	3.18	3.10	2.37
DFC	0.336	0.338	0.338

VAIO, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1700000	1700000	1700000
RC6-NIST	3380000	3330000	3350000
Rijndael	3550000	4000000	4360000
E2	4060000	4060000	4100000
E2-NIST	4860000	4960000	4950000
CRYPTON	5210000	5410000	5200000
MARS	6220000	6310000	6200000
HPC	6710000	6710000	6710000
SERPENT	7690000	7710000	7600000
CAST–256	8000000	7910000	8000000
Twofish	9520000	9210000	9300000
LOKI97	10600000	10600000	10400000
FROG	13800000	13400000	13400000
SAFER+	17600000	25000000	32000000
DEAL	21300000	21000000	27100000
MAGENTA	71300000	71900000	94500000
DFC	136000000	136000000	136000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	17.5	17.6	17.5
RC6-NIST	8.84	8.97	8.90
Rijndael	8.40	7.46	6.86
E2	7.36	7.36	7.28
E2-NIST	6.15	6.02	6.03
CRYPTON	5.73	5.52	5.75
MARS	4.80	4.74	4.82
HPC	4.45	4.45	4.45
SERPENT	3.88	3.87	3.93
CAST–256	3.73	3.78	3.73
Twofish	3.14	3.24	3.21
LOKI97	2.82	2.81	2.87
FROG	2.16	2.23	2.23
SAFER+	1.70	1.19	0.932
DEAL	1.41	1.42	1.10
MAGENTA	0.419	0.415	0.316
DFC	0.220	0.220	0.220

VAIO, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	194000	201000	194000
Rijndael	825000	864000	964000
RC6-NIST	926000	925000	939000
E2	1090000	1100000	1080000
MARS	1100000	1100000	1100000
CRYPTON	1150000	1150000	1100000
SERPENT	1150000	1150000	1150000
HPC	1200000	1200000	1200000
Twofish	1230000	1250000	1230000
LOKI97	1490000	1500000	1500000
CAST–256	1600000	1630000	1600000
E2-NIST	1700000	1710000	1730000
FROG	2010000	2010000	2050000
SAFER+	2410000	3210000	3900000
DEAL	4990000	5100000	6020000
MAGENTA	9190000	9220000	11800000
DFC	68500000	68700000	68100000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	154	149	154
Rijndael	36.2	34.6	31.0
RC6-NIST	32.2	32.3	31.8
E2	27.4	27.1	27.8
MARS	27.1	27.2	27.1
CRYPTON	26.0	25.9	27.1
SERPENT	25.9	25.9	26.0
HPC	24.8	24.9	24.8
Twofish	24.4	23.9	24.4
LOKI97	20.0	19.9	19.9
CAST–256	18.7	18.4	18.7
E2-NIST	17.5	17.4	17.3
FROG	14.9	14.9	14.6
SAFER+	12.4	9.31	7.66
DEAL	5.98	5.85	4.96
MAGENTA	3.25	3.24	2.53
DFC	0.436	0.435	0.439

VAIO, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1700000	1700000	1680000
RC6-NIST	3200000	3200000	3200000
Rijndael	3350000	3860000	4160000
E2	4160000	4160000	4160000
E2-NIST	4850000	4810000	4800000
CRYPTON	5100000	5100000	5100000
MARS	6110000	6110000	6110000
HPC	6510000	6510000	6510000
SERPENT	7510000	7510000	7510000
CAST–256	7710000	7710000	7890000
Twofish	8910000	8900000	9020000
LOKI97	10400000	10200000	10200000
FROG	13200000	13000000	13000000
SAFER+	16800000	24200000	31800000
DEAL	20200000	20200000	26000000
MAGENTA	68700000	68900000	91100000
DFC	111000000	112000000	113000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	17.5	17.6	17.8
RC6-NIST	9.32	9.32	9.32
Rijndael	8.90	7.75	7.19
E2	7.19	7.19	7.19
E2-NIST	6.16	6.21	6.22
CRYPTON	5.85	5.85	5.85
MARS	4.89	4.89	4.89
HPC	4.59	4.59	4.59
SERPENT	3.98	3.98	3.98
CAST–256	3.87	3.87	3.78
Twofish	3.35	3.36	3.31
LOKI97	2.86	2.93	2.93
FROG	2.26	2.29	2.29
SAFER+	1.77	1.23	0.938
DEAL	1.48	1.48	1.15
MAGENTA	0.435	0.433	0.328
DFC	0.269	0.266	0.265

VAIO, Linux, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1550000	1550000	1550000
RC6-NIST	2900000	2900000	2870000
Rijndael	3050000	3370000	3740000
E2	3620000	3620000	3620000
E2-NIST	4150000	4120000	4150000
CRYPTON	4590000	4580000	4580000
MARS	5370000	5400000	5390000
HPC	5770000	5780000	5790000
SERPENT	6460000	6370000	6450000
CAST–256	7070000	7030000	7050000
Twofish	8000000	7950000	7990000
LOKI97	9150000	9120000	9160000
FROG	11900000	12000000	12000000
SAFER+	14900000	21700000	28300000
DEAL	18000000	18000000	23100000
MAGENTA	62400000	62300000	82700000
DFC	111000000	111000000	111000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	19.3	19.3	19.3
RC6-NIST	10.3	10.3	10.4
Rijndael	9.79	8.86	7.98
E2	8.25	8.25	8.25
E2-NIST	7.19	7.24	7.19
CRYPTON	6.51	6.52	6.52
MARS	5.56	5.53	5.54
HPC	5.17	5.16	5.16
SERPENT	4.63	4.69	4.63
CAST–256	4.23	4.25	4.24
Twofish	3.74	3.76	3.74
LOKI97	3.26	3.28	3.26
FROG	2.50	2.48	2.49
SAFER+	2.00	1.38	1.05
DEAL	1.66	1.66	1.29
MAGENTA	0.479	0.479	0.361
DFC	0.269	0.268	0.268

VAIO, Linux, JDK 1.1.7, TYA

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	442000	441000	440000
Rijndael	1360000	1490000	1540000
RC6-NIST	1380000	1370000	1380000
E2	1640000	1630000	1600000
MARS	1910000	1990000	1900000
E2-NIST	2200000	2220000	2250000
CRYPTON	2510000	2510000	2510000
HPC	3020000	3100000	3020000
CAST–256	3370000	3460000	3400000
Twofish	4290000	4330000	4170000
FROG	4850000	4850000	4850000
SERPENT	5010000	5030000	4920000
LOKI97	5290000	5310000	5280000
DEAL	8020000	8170000	10100000
SAFER+	8620000	11700000	14800000
MAGENTA	23200000	23300000	30500000
DFC	92300000	93200000	93300000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	67.6	67.7	67.8
Rijndael	22.0	20.0	19.3
RC6-NIST	21.6	21.9	21.6
E2	18.3	18.3	18.7
MARS	15.6	15.0	15.7
E2-NIST	13.6	13.5	13.3
CRYPTON	11.9	11.9	11.9
HPC	9.89	9.62	9.89
CAST–256	8.85	8.63	8.79
Twofish	6.97	6.90	7.16
FROG	6.16	6.16	6.16
SERPENT	5.96	5.93	6.07
LOKI97	5.64	5.62	5.65
DEAL	3.73	3.66	2.96
SAFER+	3.47	2.55	2.02
MAGENTA	1.29	1.28	0.978
DFC	0.323	0.320	0.320

VAIO, Linux, JDK 1.1.7, shuJIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	415000	415000	416000
RC6-NIST	1510000	1490000	1510000
Rijndael	1540000	1680000	1720000
E2	1550000	1540000	1520000
MARS	1830000	1910000	1820000
E2-NIST	2380000	2360000	2380000
HPC	2790000	2870000	2810000
CRYPTON	3310000	3320000	3310000
LOKI97	4230000	4210000	4240000
FROG	4230000	4230000	4260000
CAST–256	4860000	4910000	4820000
Twofish	8350000	8330000	8240000
SERPENT	8600000	8580000	8480000
DEAL	9190000	9430000	11200000
SAFER+	14500000	20300000	26000000
MAGENTA	22300000	22500000	29300000
DFC	128000000	128000000	128000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	72.0	72.0	71.8
RC6-NIST	19.8	20.1	19.8
Rijndael	19.3	17.8	17.4
E2	19.3	19.4	19.6
MARS	16.3	15.6	16.4
E2-NIST	12.5	12.7	12.6
HPC	10.7	10.4	10.6
CRYPTON	9.03	8.99	9.02
LOKI97	7.06	7.09	7.04
FROG	7.06	7.06	7.01
CAST–256	6.15	6.09	6.20
Twofish	3.58	3.59	3.62
SERPENT	3.47	3.48	3.52
DEAL	3.25	3.17	2.66
SAFER+	2.06	1.47	1.15
MAGENTA	1.34	1.33	1.02
DFC	0.234	0.233	0.234

VAIO, Linux, Navigator 4.08, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	4790000	4790000	4800000
RC6-NIST	8530000	8540000	8530000
Rijndael	9310000	10400000	11500000
E2	10100000	10100000	10100000
E2-NIST	11400000	11400000	11400000
CRYPTON	13200000	13200000	13200000
MARS	15600000	15600000	15600000
HPC	16300000	16300000	16300000
CAST–256	21100000	21100000	21100000
SERPENT	21600000	21800000	21700000
Twofish	21900000	21900000	21900000
LOKI97	30700000	30700000	30600000
FROG	33700000	33800000	33700000
SAFER+	43200000	62900000	82500000
DEAL	50000000	50100000	64300000
MAGENTA	162000000	162000000	215000000
DFC	201000000	201000000	200000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	6.23	6.24	6.22
RC6-NIST	3.50	3.50	3.50
Rijndael	3.21	2.88	2.60
E2	2.96	2.96	2.95
E2-NIST	2.62	2.63	2.62
CRYPTON	2.26	2.26	2.27
MARS	1.92	1.92	1.92
HPC	1.84	1.84	1.83
CAST–256	1.41	1.42	1.42
SERPENT	1.38	1.37	1.37
Twofish	1.37	1.36	1.37
LOKI97	0.974	0.973	0.978
FROG	0.886	0.885	0.885
SAFER+	0.691	0.475	0.362
DEAL	0.598	0.596	0.465
MAGENTA	0.184	0.184	0.139
DFC	0.149	0.149	0.149

6.5 Large Blocks Decryption

6.5.1 ECB mode

We summarize the number of cycles (cycles/block) and throughput (Mbits/sec) below.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	824	854	824
E2	2200	2170	2200
RC6-NIST	6040	6200	6200
E2-NIST	6710	6710	6530
Rijndael	6900	7050	7540
MARS	7390	7350	7390
SERPENT	7900	8060	8030
CRYPTON	8060	8060	8210
HPC	8540	8730	8880
LOKI97	9030	9400	9400
CAST–256	9890	10100	10000
Twofish	9890	10200	9890
FROG	10100	10400	10400
SAFER+	13400	17500	20100
DEAL	28200	28800	33600
MAGENTA	61500	62000	83000
DFC	485000	499000	521000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	31.1	30.0	31.1
E2	11.7	11.8	11.7
RC6-NIST	4.24	4.13	4.13
E2-NIST	3.81	3.81	3.92
Rijndael	3.71	3.63	3.40
MARS	3.47	3.48	3.47
SERPENT	3.24	3.18	3.19
CRYPTON	3.18	3.18	3.12
HPC	3.00	2.93	2.88
LOKI97	2.83	2.72	2.72
CAST–256	2.59	2.54	2.55
Twofish	2.59	2.50	2.59
FROG	2.54	2.47	2.47
SAFER+	1.91	1.47	1.27
DEAL	0.908	0.889	0.763
MAGENTA	0.416	0.413	0.308
DFC	0.0527	0.0514	0.0492

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16400	16600	16400
E2	27100	27800	27200
RC6-NIST	29200	29500	29700
Rijndael	32500	35900	39600
E2-NIST	38200	38200	38600
CRYPTON	49700	50300	50200
HPC	63000	63000	63000
SERPENT	64300	63700	64300
MARS	65100	65100	64300
CAST–256	74500	74500	73700
Twofish	77800	77800	78500
LOKI97	97900	97900	97900
FROG	115000	117000	117000
SAFER+	150000	223000	287000
DEAL	196000	196000	250000
MAGENTA	686000	686000	934000
DFC	934000	945000	986000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.56	1.54	1.56
E2	0.945	0.920	0.943
RC6-NIST	0.877	0.867	0.863
Rijndael	0.788	0.713	0.647
E2-NIST	0.670	0.670	0.664
CRYPTON	0.515	0.509	0.510
HPC	0.406	0.406	0.406
SERPENT	0.398	0.402	0.398
MARS	0.393	0.393	0.398
CAST–256	0.344	0.344	0.347
Twofish	0.329	0.329	0.326
LOKI97	0.261	0.261	0.261
FROG	0.222	0.219	0.219
SAFER+	0.171	0.115	0.0892
DEAL	0.131	0.131	0.103
MAGENTA	0.0373	0.0373	0.0274
DFC	0.0274	0.0271	0.0260

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	824	1010	854
E2	2500	2350	2350
RC6-NIST	5190	5370	5190
E2-NIST	5520	5520	5550
Rijndael	5860	6040	6380
MARS	6230	6380	6200
SERPENT	6870	6900	7020
HPC	7200	7540	7390
CRYPTON	7570	7390	7540
LOKI97	8360	8730	8420
Twofish	8540	8540	8730
CAST–256	9060	9220	9060
FROG	9400	9340	9030
SAFER+	13300	16800	20000
DEAL	30800	30800	38300
MAGENTA	59100	59100	80600
DFC	333000	343000	359000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	31.1	25.4	30.0
E2	10.2	10.9	10.9
RC6-NIST	4.93	4.77	4.93
E2-NIST	4.63	4.63	4.61
Rijndael	4.37	4.24	4.01
MARS	4.11	4.01	4.13
SERPENT	3.73	3.71	3.65
HPC	3.55	3.40	3.47
CRYPTON	3.38	3.47	3.40
LOKI97	3.06	2.93	3.04
Twofish	3.00	3.00	2.93
CAST–256	2.82	2.78	2.82
FROG	2.72	2.74	2.83
SAFER+	1.92	1.52	1.28
DEAL	0.832	0.832	0.668
MAGENTA	0.433	0.433	0.318
DFC	0.0770	0.0746	0.0712

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16300	16200	16400
RC6-NIST	26800	27200	27000
E2	26900	26800	27200
Rijndael	30800	34200	37800
E2-NIST	35500	36200	35900
CRYPTON	48200	49000	48300
HPC	61000	61600	61000
SERPENT	61600	61600	62400
MARS	63600	64500	63700
CAST–256	72400	73100	73700
Twofish	75800	75700	75800
LOKI97	95200	97900	95200
FROG	118000	117000	117000
SAFER+	150000	220000	287000
DEAL	193000	196000	247000
MAGENTA	664000	676000	902000
DFC	740000	752000	771000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.57	1.58	1.56
RC6-NIST	0.954	0.943	0.949
E2	0.953	0.955	0.943
Rijndael	0.831	0.748	0.677
E2-NIST	0.721	0.707	0.713
CRYPTON	0.531	0.523	0.530
HPC	0.419	0.415	0.419
SERPENT	0.415	0.415	0.410
MARS	0.403	0.397	0.402
CAST–256	0.354	0.350	0.347
Twofish	0.338	0.338	0.338
LOKI97	0.269	0.261	0.269
FROG	0.217	0.219	0.219
SAFER+	0.171	0.116	0.0893
DEAL	0.132	0.131	0.104
MAGENTA	0.0386	0.0379	0.0284
DFC	0.0346	0.0340	0.0332

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1760	1790	1780
E2	4260	4310	4220
RC6-NIST	7840	7910	7940
Rijndael	9580	10000	10400
E2-NIST	10100	10500	10900
MARS	10700	10700	10500
SERPENT	12300	12400	12400
HPC	12400	12200	12300
CRYPTON	12600	12800	12700
Twofish	14700	14700	14800
CAST–256	17400	17500	17900
LOKI97	19100	19100	19100
FROG	25000	25500	26100
SAFER+	31300	41800	54400
DEAL	42100	42500	52000
MAGENTA	118000	117000	153000
DFC	403000	406000	427000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	21.6	21.2	21.3
E2	8.91	8.80	8.99
RC6-NIST	4.84	4.80	4.78
Rijndael	3.96	3.80	3.66
E2-NIST	3.76	3.62	3.47
MARS	3.56	3.56	3.60
SERPENT	3.08	3.07	3.07
HPC	3.07	3.11	3.08
CRYPTON	3.02	2.97	3.00
Twofish	2.58	2.58	2.57
CAST–256	2.18	2.17	2.12
LOKI97	1.99	1.99	1.98
FROG	1.52	1.49	1.46
SAFER+	1.21	0.909	0.697
DEAL	0.902	0.893	0.730
MAGENTA	0.322	0.323	0.248
DFC	0.0941	0.0935	0.0889

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	24700	24700	24700
E2	32800	32500	32400
RC6-NIST	33600	33700	34100
Rijndael	36500	39900	44000
E2-NIST	42300	42500	43900
CRYPTON	50900	50700	50600
MARS	61500	60300	61000
HPC	63200	62300	63500
CAST–256	79600	79000	79400
SERPENT	81200	82600	82100
Twofish	84500	83300	82600
LOKI97	96400	97100	97000
FROG	130000	130000	130000
SAFER+	177000	259000	342000
DEAL	207000	208000	264000
MAGENTA	641000	642000	853000
DFC	739000	769000	789000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.54	1.54	1.54
E2	1.16	1.17	1.17
RC6-NIST	1.13	1.13	1.12
Rijndael	1.04	0.953	0.864
E2-NIST	0.897	0.893	0.865
CRYPTON	0.746	0.749	0.751
MARS	0.618	0.630	0.622
HPC	0.601	0.610	0.598
CAST–256	0.477	0.480	0.478
SERPENT	0.468	0.460	0.462
Twofish	0.449	0.456	0.459
LOKI97	0.394	0.391	0.391
FROG	0.291	0.292	0.293
SAFER+	0.215	0.147	0.111
DEAL	0.184	0.183	0.144
MAGENTA	0.0592	0.0592	0.0445
DFC	0.0514	0.0493	0.0481

6.5.2 CBC mode

We summarize the number of cycles (cycles/block) and throughput (Mbits/sec) below.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	854	1010	824
E2	2350	2200	2350
RC6-NIST	8360	8390	8390
E2-NIST	9060	9060	9030
Rijndael	9220	9370	9740
MARS	9700	9700	9740
SERPENT	9700	9890	9890
CRYPTON	11000	11100	10600
HPC	11100	11400	11400
LOKI97	11400	11400	11400
Twofish	11700	11900	11700
CAST–256	11900	11900	11900
FROG	12400	13100	12800
SAFER+	15500	18800	22800
DEAL	27500	28100	35500
MAGENTA	64500	64500	85400
DFC	488000	502000	525000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	30.0	25.4	31.1
E2	10.9	11.7	10.9
RC6-NIST	3.06	3.05	3.05
E2-NIST	2.82	2.82	2.83
Rijndael	2.78	2.73	2.63
MARS	2.64	2.64	2.63
SERPENT	2.64	2.59	2.59
CRYPTON	2.32	2.31	2.42
HPC	2.31	2.24	2.25
LOKI97	2.26	2.24	2.24
Twofish	2.18	2.15	2.18
CAST–256	2.15	2.15	2.15
FROG	2.07	1.96	2.01
SAFER+	1.65	1.36	1.12
DEAL	0.932	0.912	0.721
MAGENTA	0.397	0.397	0.300
DFC	0.0524	0.0510	0.0487

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	17100	17100	16900
E2	31600	31900	31500
RC6-NIST	34500	34700	34500
Rijndael	38200	41900	45200
E2-NIST	43900	43900	43900
CRYPTON	55700	54900	55100
HPC	68400	69100	68400
SERPENT	69700	69700	69800
MARS	69700	70400	70400
CAST–256	79200	79700	79100
Twofish	83700	83900	83700
LOKI97	103000	104000	104000
FROG	123000	122000	122000
SAFER+	158000	225000	292000
DEAL	201000	201000	258000
MAGENTA	697000	697000	924000
DFC	922000	945000	986000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.50	1.50	1.51
E2	0.811	0.804	0.813
RC6-NIST	0.741	0.738	0.741
Rijndael	0.670	0.611	0.566
E2-NIST	0.583	0.583	0.583
CRYPTON	0.460	0.466	0.465
HPC	0.374	0.371	0.374
SERPENT	0.367	0.367	0.367
MARS	0.367	0.363	0.363
CAST–256	0.323	0.321	0.324
Twofish	0.306	0.305	0.306
LOKI97	0.248	0.245	0.245
FROG	0.208	0.210	0.210
SAFER+	0.162	0.114	0.0875
DEAL	0.127	0.127	0.0993
MAGENTA	0.0367	0.0367	0.0277
DFC	0.0278	0.0271	0.0260

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	824	1010	1010
E2	2320	2500	2530
RC6-NIST	6870	6870	7020
E2-NIST	7690	7690	7900
Rijndael	8030	8540	8730
SERPENT	8880	9030	9060
MARS	9400	9220	9060
HPC	9400	9550	9740
CRYPTON	9890	10100	10100
Twofish	10400	10400	10600
LOKI97	10700	10400	10700
CAST–256	11200	11600	11200
FROG	11700	11700	11700
SAFER+	15400	19500	22100
DEAL	32200	32800	39600
MAGENTA	62000	62000	83000
DFC	340000	354000	359000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	31.1	25.4	25.4
E2	11.0	10.2	10.1
RC6-NIST	3.73	3.73	3.65
E2-NIST	3.33	3.33	3.24
Rijndael	3.19	3.00	2.93
SERPENT	2.88	2.83	2.82
MARS	2.72	2.78	2.82
HPC	2.72	2.68	2.63
CRYPTON	2.59	2.54	2.54
Twofish	2.46	2.46	2.42
LOKI97	2.38	2.47	2.38
CAST–256	2.28	2.21	2.28
FROG	2.18	2.18	2.18
SAFER+	1.66	1.31	1.16
DEAL	0.794	0.780	0.647
MAGENTA	0.413	0.413	0.308
DFC	0.0752	0.0723	0.0712

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	16800	16900	16800
E2	31500	31500	31500
RC6-NIST	32000	32200	31900
Rijndael	36300	39600	42900
E2-NIST	41300	41200	41300
CRYPTON	53600	53600	54300
HPC	66300	67100	66300
SERPENT	67100	67000	67000
MARS	69000	69800	69000
CAST–256	78500	78500	79100
Twofish	80600	80400	80400
LOKI97	101000	101000	101000
FROG	124000	124000	123000
SAFER+	156000	223000	295000
DEAL	193000	196000	250000
MAGENTA	676000	676000	900000
DFC	750000	762000	783000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.53	1.51	1.53
E2	0.813	0.813	0.813
RC6-NIST	0.800	0.796	0.804
Rijndael	0.706	0.647	0.597
E2-NIST	0.620	0.621	0.620
CRYPTON	0.478	0.478	0.471
HPC	0.386	0.381	0.386
SERPENT	0.381	0.382	0.382
MARS	0.371	0.367	0.371
CAST–256	0.326	0.326	0.324
Twofish	0.318	0.318	0.318
LOKI97	0.255	0.255	0.255
FROG	0.207	0.207	0.208
SAFER+	0.164	0.115	0.0868
DEAL	0.133	0.131	0.103
MAGENTA	0.0379	0.0379	0.0284
DFC	0.0341	0.0336	0.0327

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1790	1810	1810
E2	4590	4700	4530
RC6-NIST	10700	10600	10700
Rijndael	12200	12900	13400
MARS	13500	13700	13600
E2-NIST	13600	13600	14200
HPC	14900	14900	15000
CRYPTON	15200	15200	15300
SERPENT	16700	16600	16600
Twofish	17900	17900	17900
CAST–256	20000	21200	20400
LOKI97	25300	25300	24600
FROG	27800	27600	28400
SAFER+	33800	45800	57000
DEAL	46100	45900	55000
MAGENTA	121000	121000	160000
DFC	403000	416000	427000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	21.2	21.0	21.0
E2	8.26	8.07	8.38
RC6-NIST	3.57	3.58	3.57
Rijndael	3.11	2.94	2.84
MARS	2.81	2.77	2.79
E2-NIST	2.79	2.79	2.67
HPC	2.54	2.54	2.53
CRYPTON	2.50	2.50	2.49
SERPENT	2.28	2.29	2.29
Twofish	2.12	2.12	2.12
CAST–256	1.90	1.79	1.86
LOKI97	1.50	1.50	1.54
FROG	1.36	1.37	1.34
SAFER+	1.12	0.830	0.666
DEAL	0.823	0.827	0.691
MAGENTA	0.314	0.313	0.237
DFC	0.0942	0.0912	0.0889

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	25500	25600	25500
E2	37000	36500	36500
RC6-NIST	40500	40600	41100
Rijndael	42500	46700	51100
E2-NIST	49300	49100	49700
CRYPTON	56800	56400	56700
HPC	69600	69900	69700
MARS	70700	71300	70500
CAST–256	81900	82400	82000
SERPENT	89100	87900	87800
Twofish	90100	89900	89700
LOKI97	103000	105000	102000
FROG	136000	138000	136000
SAFER+	184000	266000	347000
DEAL	212000	213000	271000
MAGENTA	649000	650000	878000
DFC	748000	757000	784000

Throughput (Mbits/sec)

Key length (bit)	128	192	256
RC6	1.49	1.48	1.49
E2	1.03	1.04	1.04
RC6-NIST	0.938	0.936	0.924
Rijndael	0.894	0.813	0.743
E2-NIST	0.770	0.773	0.765
CRYPTON	0.668	0.674	0.670
HPC	0.546	0.544	0.545
MARS	0.537	0.533	0.538
CAST–256	0.464	0.461	0.463
SERPENT	0.426	0.432	0.432
Twofish	0.422	0.422	0.423
LOKI97	0.369	0.363	0.371
FROG	0.278	0.276	0.280
SAFER+	0.206	0.143	0.109
DEAL	0.179	0.178	0.140
MAGENTA	0.0585	0.0584	0.0432
DFC	0.0508	0.0502	0.0484

6.5.3 1-bit CFB mode

We summarize the number of cycles (cycles/block) and throughput (Kbits/sec) below. Note that the unit of throughput differs from that for the ECB and CBC modes.

NIST, Win95, JDK 1.2, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	91800	96700	90800
E2	301000	311000	301000
RC6-NIST	719000	719000	719000
E2-NIST	814000	816000	814000
Rijndael	814000	869000	912000
MARS	883000	902000	879000
SERPENT	922000	902000	922000
CRYPTON	965000	969000	965000
HPC	1010000	1010000	988000
LOKI97	1120000	1120000	1120000
CAST–256	1180000	1180000	1200000
Twofish	1200000	1200000	1200000
FROG	1590000	1550000	1590000
SAFER+	1630000	1980000	2410000
DEAL	3530000	3610000	4380000
MAGENTA	7380000	7560000	9590000
DFC	57800000	55600000	60300000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	279	265	282
E2	85.1	82.4	85.1
RC6-NIST	35.6	35.6	35.6
E2-NIST	31.4	31.4	31.4
Rijndael	31.4	29.5	28.1
MARS	29.0	28.4	29.1
SERPENT	27.8	28.4	27.8
CRYPTON	26.5	26.4	26.5
HPC	25.4	25.4	25.9
LOKI97	22.9	22.9	22.9
CAST–256	21.7	21.7	21.3
Twofish	21.3	21.3	21.3
FROG	16.1	16.5	16.1
SAFER+	15.8	12.9	10.6
DEAL	7.25	7.09	5.85
MAGENTA	3.47	3.39	2.67
DFC	0.443	0.460	0.425

NIST, Win95, JDK 1.2, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1840000	1870000	1870000
RC6-NIST	3460000	3450000	3430000
Rijndael	3910000	4380000	4840000
E2	4030000	4080000	4070000
E2-NIST	4680000	4720000	4670000
CRYPTON	6090000	6190000	6170000
HPC	7640000	7640000	7640000
SERPENT	7640000	7720000	7640000
MARS	7720000	7810000	7730000
CAST–256	9360000	9360000	9340000
Twofish	9690000	9700000	9690000
LOKI97	12200000	12300000	12400000
FROG	16700000	16600000	16700000
SAFER+	19100000	28000000	36400000
DEAL	24900000	24700000	31800000
MAGENTA	87700000	87700000	117000000
DFC	122000000	118000000	123000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.9	13.7	13.7
RC6-NIST	7.41	7.41	7.46
Rijndael	6.55	5.84	5.29
E2	6.35	6.28	6.29
E2-NIST	5.47	5.43	5.48
CRYPTON	4.20	4.14	4.15
HPC	3.35	3.35	3.35
SERPENT	3.35	3.32	3.35
MARS	3.32	3.28	3.31
CAST–256	2.74	2.74	2.74
Twofish	2.64	2.64	2.64
LOKI97	2.10	2.07	2.07
FROG	1.54	1.54	1.54
SAFER+	1.34	0.915	0.703
DEAL	1.03	1.04	0.806
MAGENTA	0.292	0.292	0.220
DFC	0.209	0.217	0.208

NIST, Win95, JDK 1.1.7, Symantec JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	91800	90800	90800
E2	311000	322000	322000
RC6-NIST	622000	628000	616000
Rijndael	654000	729000	752000
E2-NIST	676000	697000	697000
MARS	754000	750000	773000
SERPENT	813000	813000	816000
HPC	859000	836000	859000
CRYPTON	902000	902000	945000
LOKI97	984000	984000	945000
Twofish	1030000	1050000	1030000
CAST–256	1120000	1140000	1140000
FROG	1410000	1460000	1460000
SAFER+	1550000	1970000	2410000
DEAL	3340000	3340000	4110000
MAGENTA	7380000	7560000	9590000
DFC	45000000	43900000	46200000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	279	282	282
E2	82.4	79.4	79.4
RC6-NIST	41.2	40.8	41.5
Rijndael	39.1	35.1	34.0
E2-NIST	37.9	36.7	36.7
MARS	34.0	34.1	33.1
SERPENT	31.5	31.5	31.4
HPC	29.8	30.6	29.8
CRYPTON	28.4	28.4	27.1
LOKI97	26.0	26.0	27.1
Twofish	24.8	24.4	24.9
CAST–256	22.9	22.5	22.5
FROG	18.1	17.5	17.5
SAFER+	16.5	13.0	10.6
DEAL	7.66	7.66	6.23
MAGENTA	3.47	3.39	2.67
DFC	0.569	0.583	0.555

NIST, Win95, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	1890000	1910000	1890000
RC6-NIST	3260000	3260000	3260000
Rijndael	3770000	4200000	4630000
E2	4030000	4040000	4030000
E2-NIST	4550000	4550000	4590000
CRYPTON	5920000	6020000	5920000
HPC	7470000	7470000	7470000
SERPENT	7560000	7550000	7550000
MARS	7640000	7720000	7640000
CAST–256	9090000	9190000	9170000
Twofish	9440000	9440000	9440000
LOKI97	12200000	12200000	12200000
FROG	16800000	16700000	16800000
SAFER+	19000000	27800000	36400000
DEAL	24400000	24200000	31400000
MAGENTA	85300000	85500000	114000000
DFC	97700000	94800000	98500000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.6	13.4	13.6
RC6-NIST	7.86	7.85	7.85
Rijndael	6.78	6.09	5.53
E2	6.35	6.34	6.35
E2-NIST	5.62	5.63	5.57
CRYPTON	4.32	4.26	4.32
HPC	3.43	3.43	3.43
SERPENT	3.39	3.39	3.39
MARS	3.35	3.32	3.35
CAST–256	2.82	2.79	2.79
Twofish	2.71	2.71	2.71
LOKI97	2.10	2.10	2.10
FROG	1.52	1.54	1.52
SAFER+	1.35	0.920	0.703
DEAL	1.05	1.06	0.815
MAGENTA	0.300	0.300	0.225
DFC	0.262	0.270	0.260

UE450, SunOS 5.6, JDK 1.1.7, Sun JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	184000	184000	183000
E2	578000	636000	623000
RC6-NIST	982000	979000	974000
Rijndael	1110000	1250000	1270000
MARS	1260000	1220000	1260000
E2-NIST	1290000	1170000	1200000
HPC	1520000	1480000	1520000
SERPENT	1520000	1530000	1520000
CRYPTON	1540000	1560000	1540000
Twofish	2060000	1870000	1890000
CAST–256	2210000	2250000	2180000
LOKI97	2440000	2430000	2460000
FROG	3190000	3350000	3160000
SAFER+	4140000	5550000	7280000
DEAL	5320000	5470000	6570000
MAGENTA	15100000	15200000	19900000
DFC	53500000	51700000	55200000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	206	206	207
E2	65.7	59.7	61.0
RC6-NIST	38.7	38.8	39.0
Rijndael	34.2	30.5	29.9
MARS	30.2	31.0	30.2
E2-NIST	29.4	32.5	31.5
HPC	25.0	25.6	25.0
SERPENT	24.9	24.8	25.0
CRYPTON	24.7	24.3	24.6
Twofish	18.5	20.3	20.1
CAST–256	17.2	16.8	17.4
LOKI97	15.5	15.6	15.5
FROG	11.9	11.4	12.0
SAFER+	9.17	6.85	5.22
DEAL	7.14	6.95	5.78
MAGENTA	2.52	2.50	1.91
DFC	0.709	0.735	0.687

UE450, SunOS 5.6, JDK 1.1.7, w/o JIT

Number of cycles (cycles/block)

Key length (bit)	128	192	256
RC6	2900000	2860000	2840000
RC6-NIST	4320000	4300000	4360000
Rijndael	4510000	5010000	5600000
E2	4810000	4830000	4860000
E2-NIST	5470000	5480000	5460000
CRYPTON	6730000	6730000	6730000
HPC	7870000	7730000	7890000
MARS	8000000	7850000	7930000
CAST–256	9960000	9890000	9990000
SERPENT	10200000	10300000	10200000
Twofish	10500000	10700000	10500000
LOKI97	12300000	12400000	12300000
FROG	17400000	17400000	17400000
SAFER+	22700000	33000000	43500000
DEAL	25500000	25300000	32800000
MAGENTA	82300000	82300000	109000000
DFC	99700000	97100000	101000000

Throughput (Kbits/sec)

Key length (bit)	128	192	256
RC6	13.1	13.3	13.4
RC6-NIST	8.79	8.83	8.72
Rijndael	8.42	7.58	6.78
E2	7.89	7.87	7.81
E2-NIST	6.94	6.93	6.95
CRYPTON	5.64	5.64	5.64
HPC	4.82	4.91	4.81
MARS	4.75	4.84	4.79
CAST–256	3.81	3.84	3.80
SERPENT	3.73	3.69	3.74
Twofish	3.62	3.54	3.61
LOKI97	3.08	3.07	3.08
FROG	2.18	2.18	2.18
SAFER+	1.68	1.15	0.873
DEAL	1.49	1.50	1.16
MAGENTA	0.462	0.461	0.348
DFC	0.381	0.391	0.375