電腦安全概論

組員:108316107 龍昱璇
108316121 朱家儀
108316122 簡昕儀

Windows DES執行效能

```
C:\Program Files\OpenSSL-Win64\bin>openssl speed des
Doing des-ede3 for 3s on 16 size blocks: 7367362 des-ede3's in 3.02s
Doing des-ede3 for 3s on 64 size blocks: 1873463 des-ede3's in 3.00s
Doing des-ede3 for 3s on 256 size blocks: 470132 des-ede3's in 3.00s
Doing des-ede3 for 3s on 1024 size blocks: 117549 des-ede3's in 3.00s
Doing des-ede3 for 3s on 8192 size blocks: 14818 des-ede3's in 3.02s
Doing des-ede3 for 3s on 16384 size blocks: 7428 des-ede3's in 3.00s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7daf3fffebffff:0x405d4ef2bf67eb
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
des-cbc              0.00         0.00         0.00         0.00         0.00         0.00
des-ede3         39089.01k    39967.21k    40117.93k    40123.39k    40253.37k    40566.78k
48100000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:unsupported:crypto\evp\evp_fetch.c:341:Global default library context, Algorithm (DES-CBC : 13), Properties ()
```

Ubuntu DES執行效能

```
ubuntu@ubuntu:~/DES$ openssl speed des
Doing des-ede3 for 3s on 16 size blocks: 7062549 des-ede3's in 2.99s
Doing des-ede3 for 3s on 64 size blocks: 1742641 des-ede3's in 3.00s
Doing des-ede3 for 3s on 256 size blocks: 443077 des-ede3's in 3.00s
Doing des-ede3 for 3s on 1024 size blocks: 112217 des-ede3's in 2.99s
Doing des-ede3 for 3s on 8192 size blocks: 13992 des-ede3's in 3.00s
Doing des-ede3 for 3s on 16384 size blocks: 7041 des-ede3's in 3.00s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
des-cbc              0.00         0.00         0.00         0.00         0.00
        0.00
des-ede3         37792.90k    37176.34k    37809.24k    38431.51k    38207.49k
   38453.25k
40974A05167F0000:error:0308010C:digital envelope routines:inner_evp_generic_fet
ch:unsupported:../crypto/evp/evp_fetch.c:349:Global default library context, Al
gorithm (DES-CBC : 7), Properties ()
```

openssl speed AES

```
C:\Program Files\OpenSSL-Win64\bin>openssl speed aes
Doing aes-128-cbc for 3s on 16 size blocks: 70525442 aes-128-cbc's in 3.00s
Doing aes-128-cbc for 3s on 64 size blocks: 19635995 aes-128-cbc's in 3.02s
Doing aes-128-cbc for 3s on 256 size blocks: 5054014 aes-128-cbc's in 3.00s
Doing aes-128-cbc for 3s on 1024 size blocks: 1279739 aes-128-cbc's in 3.02s
Doing aes-128-cbc for 3s on 8192 size blocks: 160668 aes-128-cbc's in 3.02s
Doing aes-128-cbc for 3s on 16384 size blocks: 80694 aes-128-cbc's in 3.00s
Doing aes-192-cbc for 3s on 16 size blocks: 61687693 aes-192-cbc's in 3.00s
Doing aes-192-cbc for 3s on 64 size blocks: 16645542 aes-192-cbc's in 3.02s
Doing aes-192-cbc for 3s on 256 size blocks: 4235304 aes-192-cbc's in 3.02s
Doing aes-192-cbc for 3s on 1024 size blocks: 1076092 aes-192-cbc's in 3.02s
Doing aes-192-cbc for 3s on 8192 size blocks: 135030 aes-192-cbc's in 3.02s
Doing aes-192-cbc for 3s on 16384 size blocks: 66821 aes-192-cbc's in 3.02s
Doing aes-256-cbc for 3s on 16 size blocks: 52381664 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 64 size blocks: 14325625 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 256 size blocks: 3618167 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 1024 size blocks: 913998 aes-256-cbc's in 3.02s
Doing aes-256-cbc for 3s on 8192 size blocks: 114043 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 16384 size blocks: 57425 aes-256-cbc's in 3.02s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: ba(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7dfaf3ffffebffff:0x4054ef2bf67eb
The 'numbers' are in 1000s of bytes per second processed.
type          16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-cbc     376135.69k   416730.75k   431275.86k   434554.28k   436457.54k   440696.83k
aes-192-cbc     329001.03k   353264.97k   359540.00k   365402.93k   366811.44k   363040.92k
aes-256-cbc     279368.87k   305613.33k   308750.25k   310361.52k   311413.42k   311992.11k
```

Ubuntu AES執行效能

```
ubuntu@ubuntu:~/AES$ openssl speed aes
Doing aes-128-cbc for 3s on 16 size blocks: 75050678 aes-128-cbc's in 2.99s
Doing aes-128-cbc for 3s on 64 size blocks: 19380448 aes-128-cbc's in 3.00s
Doing aes-128-cbc for 3s on 256 size blocks: 4883106 aes-128-cbc's in 2.99s
Doing aes-128-cbc for 3s on 1024 size blocks: 1217282 aes-128-cbc's in 3.00s
Doing aes-128-cbc for 3s on 8192 size blocks: 151600 aes-128-cbc's in 2.99s
Doing aes-128-cbc for 3s on 16384 size blocks: 76014 aes-128-cbc's in 3.00s
Doing aes-192-cbc for 3s on 16 size blocks: 62840999 aes-192-cbc's in 2.99s
Doing aes-192-cbc for 3s on 64 size blocks: 16185596 aes-192-cbc's in 3.00s
Doing aes-192-cbc for 3s on 256 size blocks: 4018801 aes-192-cbc's in 3.00s
Doing aes-192-cbc for 3s on 1024 size blocks: 1017501 aes-192-cbc's in 2.99s
Doing aes-192-cbc for 3s on 8192 size blocks: 127037 aes-192-cbc's in 3.00s
Doing aes-192-cbc for 3s on 16384 size blocks: 63552 aes-192-cbc's in 3.00s
Doing aes-256-cbc for 3s on 16 size blocks: 54392840 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 64 size blocks: 13932752 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 256 size blocks: 3473394 aes-256-cbc's in 2.99s
Doing aes-256-cbc for 3s on 1024 size blocks: 875107 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 8192 size blocks: 109517 aes-256-cbc's in 3.00s
Doing aes-256-cbc for 3s on 16384 size blocks: 54709 aes-256-cbc's in 3.00s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
```

```
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
aes-128-cbc     401608.98k   413449.56k   418085.33k   415498.92k   415353.58k
  415137.79k
aes-192-cbc     336272.90k   345292.71k   342937.69k   348468.57k   346895.70k
  347078.66k
aes-256-cbc     290095.15k   297232.04k   297387.58k   298703.19k   299054.42k
  298784.09k
```

效能分析

單位:Block	Windows	Linux	效能差異
DES-ede3 (blocks/3 sec)	7428	7041	387
AES-256-cbc (blocks/3 sec)	57425	54709	2716

DES的效能比AES好，AES較安全

Windows MD5

```
C:\Program Files\OpenSSL-Win64\bin>openssl speed md5
Doing md5 for 3s on 16 size blocks: 12796048 md5's in 3.02s
Doing md5 for 3s on 64 size blocks: 10021324 md5's in 3.02s
Doing md5 for 3s on 256 size blocks: 5980307 md5's in 3.02s
Doing md5 for 3s on 1024 size blocks: 2307308 md5's in 3.02s
Doing md5 for 3s on 8192 size blocks: 344008 md5's in 3.02s
Doing md5 for 3s on 16384 size blocks: 174318 md5's in 3.02s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7daf3ffffebffff:0x405d4ef2bf67eb
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
md5              67891.99k   212680.53k   507675.39k   783480.50k   934503.97k   947076.02k
```

計算Hash值，執行效能

Ubuntu md5

```
ubuntu@ubuntu:~$ md5sum d.txt
e59ff97941044f85df5297e1c302d260  d.txt
ubuntu@ubuntu:~$ openssl speed md5
Doing md5 for 3s on 16 size blocks: 21283944 md5's in 2.99s
Doing md5 for 3s on 64 size blocks: 14255182 md5's in 3.00s
Doing md5 for 3s on 256 size blocks: 7264460 md5's in 2.99s
Doing md5 for 3s on 1024 size blocks: 2463508 md5's in 3.00s
Doing md5 for 3s on 8192 size blocks: 343916 md5's in 3.00s
Doing md5 for 3s on 16384 size blocks: 171992 md5's in 3.00s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
md5             113894.01k   304110.55k   621973.83k   840877.40k   939119.96k
  939305.64k
```

Windows SHA-1

```
C:\Program Files\OpenSSL-Win64\bin>openssl speed sha1
Doing sha1 for 3s on 16 size blocks: 14109895 sha1's in 3.00s
Doing sha1 for 3s on 64 size blocks: 12673604 sha1's in 3.02s
Doing sha1 for 3s on 256 size blocks: 9315972 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 4569147 sha1's in 3.00s
Doing sha1 for 3s on 8192 size blocks: 775143 sha1's in 3.02s
Doing sha1 for 3s on 16384 size blocks: 393860 sha1's in 3.02s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7dfaf3ffffebffff:0x405d4ef2bf67eb
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
sha1             75252.77k   268969.34k   794962.94k  1559602.18k  2105690.02k  2139855.67k
```

計算Hash值，執行效能

Ubuntu SHA-1

```
ubuntu@ubuntu:~$ sha1sum d.txt
648a6a6ffffdaa0badb23b8baf90b6168dd16b3a  d.txt
ubuntu@ubuntu:~$ openssl speed sha1
Doing sha1 for 3s on 16 size blocks: 21205151 sha1's in 2.99s
Doing sha1 for 3s on 64 size blocks: 14642485 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 8139380 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 2956643 sha1's in 2.99s
Doing sha1 for 3s on 8192 size blocks: 428860 sha1's in 3.00s
Doing sha1 for 3s on 16384 size blocks: 215141 sha1's in 2.99s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
sha1           113472.38k   312373.01k   694560.43k  1012576.06k  1171073.71k
 1178886.34k
```

Windows SHA-256

```
C:\Program Files\OpenSSL-Win64\bin>openssl speed sha256
Doing sha256 for 3s on 16 size blocks: 14196092 sha256's in 3.00s
Doing sha256 for 3s on 64 size blocks: 12285368 sha256's in 3.02s
Doing sha256 for 3s on 256 size blocks: 8674645 sha256's in 3.00s
Doing sha256 for 3s on 1024 size blocks: 3995531 sha256's in 3.00s
Doing sha256 for 3s on 8192 size blocks: 663965 sha256's in 3.02s
Doing sha256 for 3s on 16384 size blocks: 339751 sha256's in 3.02s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7daf3ffffebffff:0x405d4ef2bf67eb
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
sha256           75712.49k   260729.88k   740236.37k  1363807.91k  1803672.96k  1845879.51k
```

Ubuntu SHA-256

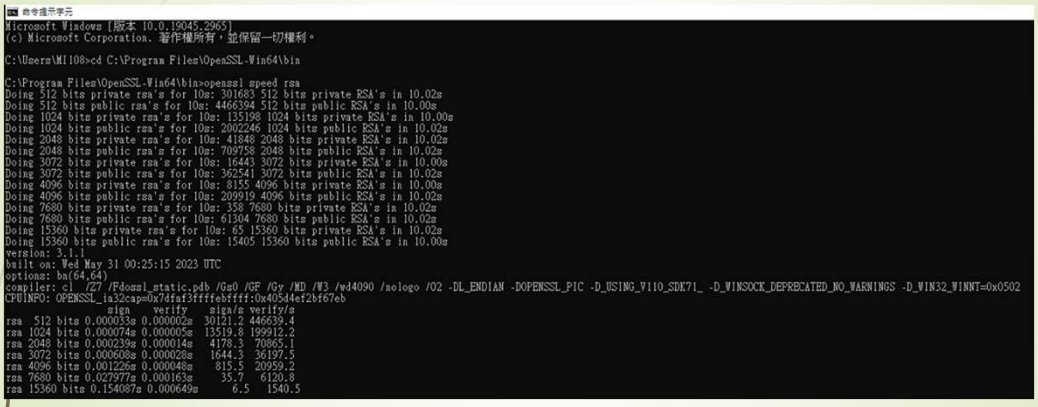
```
ubuntu@ubuntu:~$ sha256sum d.txt
d2a84f4b8b650937ec8f73cd8be2c74add5a911ba64df27458ed8229da804a26  d.txt
ubuntu@ubuntu:~$ openssl speed sha256
Doing sha256 for 3s on 16 size blocks: 13859793 sha256's in 3.00s
Doing sha256 for 3s on 64 size blocks: 8767299 sha256's in 3.00s
Doing sha256 for 3s on 256 size blocks: 4338213 sha256's in 3.00s
Doing sha256 for 3s on 1024 size blocks: 1413735 sha256's in 3.00s
Doing sha256 for 3s on 8192 size blocks: 196528 sha256's in 2.99s
Doing sha256 for 3s on 16384 size blocks: 98355 sha256's in 3.00s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
sha256           73918.90k   187035.71k   370194.18k   482554.88k   538447.28k
  537149.44k
```

執行效能

單位:Block	Windows	Linux	效能差異
MD5 (blocks/3 sec)	174318	171992	2326
SHA-1 (blocks/3 sec)	393860	215141	178719
SHA-256 (blocks/3 sec)	339751	98355	241396

MD5容易破解，sha256安全性最高

Windows RSA執行效能



```
命令提示字元
Microsoft Windows [版本 10.0.19045.2965]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\MI108>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>openssl speed rsa
Doing 512 bits private rsa's for 10s: 301683 512 bits private RSA's in 10.02s
Doing 512 bits public rsa's for 10s: 4466384 512 bits public RSA's in 10.00s
Doing 1024 bits private rsa's for 10s: 135198 1024 bits private RSA's in 10.00s
Doing 1024 bits public rsa's for 10s: 2002246 1024 bits public RSA's in 10.02s
Doing 2048 bits private rsa's for 10s: 41848 2048 bits private RSA's in 10.02s
Doing 2048 bits public rsa's for 10s: 709758 2048 bits public RSA's in 10.02s
Doing 3072 bits private rsa's for 10s: 16443 3072 bits private RSA's in 10.00s
Doing 3072 bits public rsa's for 10s: 362541 3072 bits public RSA's in 10.02s
Doing 4096 bits private rsa's for 10s: 8155 4096 bits private RSA's in 10.00s
Doing 4096 bits public rsa's for 10s: 209919 4096 bits public RSA's in 10.02s
Doing 7680 bits private rsa's for 10s: 358 7680 bits private RSA's in 10.02s
Doing 7680 bits public rsa's for 10s: 61304 7680 bits public RSA's in 10.02s
Doing 15360 bits private rsa's for 10s: 65 15360 bits private RSA's in 10.02s
Doing 15360 bits public rsa's for 10s: 15405 15360 bits public RSA's in 10.00s
version: 3.1.1
built on: Wed May 31 00:25:15 2023 UTC
options: bn(64,64)
compiler: cl /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D_USING_V110_SDK71_ -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0x7dfaf3fffffebffff:0x40544ef2bf67eb
                  sign    verify    sign/s verify/s
rsa  512 bits 0.000033s 0.000002s  30121.2 446639.4
rsa 1024 bits 0.000074s 0.000005s  13519.8 199912.2
rsa 2048 bits 0.000239s 0.000014s   4178.3  70865.1
rsa 3072 bits 0.000608s 0.000028s   1644.3  36197.5
rsa 4096 bits 0.001226s 0.000048s    815.5  20959.2
rsa 7680 bits 0.027977s 0.000163s     35.7   6120.8
rsa 15360 bits 0.154087s 0.000649s     6.5   1540.5
```

RSA算法的執行效能

Ubuntu RSA的效能

```
ubuntu@ubuntu:~/rsa$ openssl speed rsa
Doing 512 bits private rsa's for 10s: 377567 512 bits private RSA's in 9.99s
Doing 512 bits public rsa's for 10s: 5296908 512 bits public RSA's in 9.99s
Doing 1024 bits private rsa's for 10s: 116350 1024 bits private RSA's in 9.99s
Doing 1024 bits public rsa's for 10s: 1903760 1024 bits public RSA's in 9.98s
Doing 2048 bits private rsa's for 10s: 22634 2048 bits private RSA's in 9.99s
Doing 2048 bits public rsa's for 10s: 553827 2048 bits public RSA's in 10.00s
Doing 3072 bits private rsa's for 10s: 5127 3072 bits private RSA's in 10.00s
Doing 3072 bits public rsa's for 10s: 251739 3072 bits public RSA's in 10.00s
Doing 4096 bits private rsa's for 10s: 2239 4096 bits private RSA's in 10.00s
Doing 4096 bits public rsa's for 10s: 145129 4096 bits public RSA's in 9.99s
Doing 7680 bits private rsa's for 10s: 246 7680 bits private RSA's in 10.00s
Doing 7680 bits public rsa's for 10s: 41471 7680 bits public RSA's in 10.00s
Doing 15360 bits private rsa's for 10s: 44 15360 bits private RSA's in 10.04s
Doing 15360 bits public rsa's for 10s: 10657 15360 bits public RSA's in 10.00s
version: 3.0.2
built on: Mon Feb  6 17:57:17 2023 UTC
options: bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g
-O2 -ffile-prefix-map=/build/openssl-hnAO60/openssl-3.0.2=. -flto=auto -ffat-lt
o-objects -flto=auto -ffat-lto-objects -fstack-protector-strong -Wformat -Werro
r=format-security -DOPENSSL_TLS_SECURITY_LEVEL=2 -DOPENSSL_USE_NODELETE -DL_END
IAN -DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DNDEBUG -Wdate-time -D_FORTIFY_SO
URCE=2
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
                  sign    verify    sign/s verify/s
rsa  512 bits 0.000026s 0.000002s  37794.5 530221.0
rsa 1024 bits 0.000086s 0.000005s  11646.6 190757.5
rsa 2048 bits 0.000441s 0.000018s   2265.7  55382.7
```

```
CPUINFO: OPENSSL_ia32cap=0xdcfa2203478bffff:0x842569
                  sign    verify    sign/s verify/s
rsa  512 bits 0.000026s 0.000002s  37794.5 530221.0
rsa 1024 bits 0.000086s 0.000005s  11646.6 190757.5
rsa 2048 bits 0.000441s 0.000018s   2265.7  55382.7
rsa 3072 bits 0.001950s 0.000040s    512.7  25173.9
rsa 4096 bits 0.004466s 0.000069s    223.9  14527.4
rsa 7680 bits 0.040650s 0.000241s     24.6   4147.1
rsa 15360 bits 0.228182s 0.000938s      4.4   1065.7
```

效能分析

單位:Block	Windows	Linux	效能差異
RSA public key-15360bits (times)	15405	10657	4748
RSA private key-15360bits (times)	65	44	21

Windows裝置規格

裝置規格 複製

裝置名稱	DESKTOP-05E48CD
處理器	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
已安裝記憶體(RAM)	4.00 GB (3.85 GB 可用)
裝置識別碼	102D0DE4-B0E7-48D9-B8EE-18EB41401B1E
產品識別碼	00325-81407-84095-AAOEM
系統類型	64 位元作業系統，x64 型處理器
手寫筆與觸控	此顯示器不提供手寫筆或觸控式輸入功能

```
C:\Users\jorda>WMIC CPU Get DeviceID,NumberOfCores,NumberOfLogicalProcessors
DeviceID  NumberOfCores  NumberOfLogicalProcessors
CPU0      4              8
```

Linux cpu

```
ubuntu@ubuntu:~$ lscpu
Architecture:            x86_64
  CPU op-mode(s):        32-bit, 64-bit
  Address sizes:         39 bits physical, 48 bits virtual
  Byte Order:            Little Endian
CPU(s):                  2
  On-line CPU(s) list:   0,1
Vendor ID:               GenuineIntel
  Model name:            11th Gen Intel(R) Core(TM) i7-11700 @ 2.50GHz
    CPU family:          6
    Model:               167
    Thread(s) per core:  1
    Core(s) per socket:  2
    Socket(s):           1
    Stepping:            1
    BogoMIPS:            4991.99
    Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep m
                         ca cmov pat pse36 clflush mmx fxsr sse sse2 h
                          nx rdtscp lm constant_tsc rep_good nopl xtop
                         stop_tsc cpuid tsc_known_freq pni pclmulqdq s
                          pcid sse4_1 sse4_2 x2apic movbe popcnt xsave
                         nd hypervisor lahf_lm abm 3dnowprefetch invpc
```

結論

AES為對稱式加密演算法，執行效能更高，使用的金鑰長度較小

RSA為非對稱式加密演算法:使用的金鑰長度較長，安全性較高

DES較為不安全的演算法

MD5 存在碰撞攻擊的風險，被視為較不安全

SHA256較安全

SHA1執行效能較MD5慢一些

所使用的Windows核心數目較多，所以執行效能較linux的高