

NAME

openssl-speed, speed – test library performance

SYNOPSIS

openssl speed [**-help**] [**-engine id**] [**-elapsed**] [**-evp algo**] [**-decrypt**] [**-rand file...**] [**-writerand file**]
 [**-primes num**] [**-seconds num**] [**-bytes num**] [**algorithm...**]

DESCRIPTION

This command is used to test the performance of cryptographic algorithms. To see the list of supported algorithms, use the *list --digest-commands* or *list --cipher-commands* command. The global CSPRNG is denoted by the *rand* algorithm name.

OPTIONS**-help**

Print out a usage message.

-engine id

Specifying an engine (by its unique **id** string) will cause **speed** to attempt to obtain a functional reference to the specified engine, thus initialising it if needed. The engine will then be set as the default for all available algorithms.

-elapsed

When calculating operations- or bytes-per-second, use wall-clock time instead of CPU user time as divisor. It can be useful when testing speed of hardware engines.

-evp algo

Use the specified cipher or message digest algorithm via the EVP interface. If **algo** is an AEAD cipher, then you can pass **<-aead>** to benchmark a TLS-like sequence. And if **algo** is a multi-buffer capable cipher, e.g. **aes-128-cbc-hmac-sha1**, then **-mb** will time multi-buffer operation.

-decrypt

Time the decryption instead of encryption. Affects only the EVP testing.

-rand file...

A file or files containing random data used to seed the random number generator. Multiple files can be specified separated by an OS-dependent character. The separator is **;** for MS-Windows, **,** for OpenVMS, and **:** for all others.

[-writerand file]

Writes random data to the specified *file* upon exit. This can be used with a subsequent **-rand** flag.

-primes num

Generate a **num**-prime RSA key and use it to run the benchmarks. This option is only effective if RSA algorithm is specified to test.

-seconds num

Run benchmarks for **num** seconds.

-bytes num

Run benchmarks on **num**-byte buffers. Affects ciphers, digests and the CSPRNG.

[zero or more test algorithms]

If any options are given, **speed** tests those algorithms, otherwise a pre-compiled grand selection is tested.

COPYRIGHT

Copyright 2000–2018 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (the “License”). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.