NAME

openssl-speed - test library performance

SYNOPSIS

openssl speed [**-help**] [**-elapsed**] [**-evp** *algo*] [**-hmac** *algo*] [**-cmac** *algo*] [**-mb**] [**-aead**] [**-multi** *num*] [**-async_jobs** *num*] [**-misalign** *num*] [**-decrypt**] [**-primes** *num*] [**-seconds** *num*] [**-bytes** *num*] [**-mr**] [**-rand** *files*] [**-writerand** *file*] [**-engine** *id*] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*] [*algorithm* ...]

DESCRIPTION

This command is used to test the performance of cryptographic algorithms.

OPTIONS

-help

Print out a usage message.

-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.

To see the algorithms supported with this option, use "openssl list -digest-algorithms" or "openssl list -cipher-algorithms" command.

-multi *num*

Run multiple operations in parallel.

-async_jobs *num*

Enable async mode and start specified number of jobs.

-misalign *num*

Misalign the buffers by the specified number of bytes.

-hmac *digest*

Time the HMAC algorithm using the specified message digest.

-cmac *cipher*
Time the CMAC algorithm using the specified cipher e.g. "openssl speed -cmac aes128".

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

-mb Enable multi-block mode on EVP-named cipher.

-aead
Benchmark EVP-named AEAD cipher in TLS-like sequence.

-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. The limit on the size of the buffer is INT_MAX - 64 bytes, which for a 32-bit int would be 2147483583 bytes.

-mr Produce the summary in a mechanical, machine-readable, format.

-rand *files*, **-writerand** *file*
See "Random State Options" in **openssl**(1) for details.

-engine *id*
See "Engine Options" in **openssl**(1). This option is deprecated.

-provider *name*
-provider-path *path*
-propquery *propq*
See "Provider Options" in **openssl**(1), **provider**(7), and **property**(7).

algorithm ...
If any *algorithm* is given, then those algorithms are tested, otherwise a pre-compiled grand selection is tested.

BUGS

The *algorithm* can be selected only from a pre-compiled subset of things that the "openssl speed" command knows about. To test any additional digest or cipher algorithm supported by OpenSSL use the "-evp" option.

There is no way to test the speed of any additional public key algorithms supported by third party providers with the "openssl speed" command.

HISTORY

The **-engine** option was deprecated in OpenSSL 3.0.

COPYRIGHT