

**NAME**

openssl-rand, rand – generate pseudo-random bytes

**SYNOPSIS**

**openssl rand** [**-help**] [**-out** *file*] [**-rand** *file...*] [**-writerand** *file*] [**-base64**] [**-hex**] *num*

**DESCRIPTION**

The **rand** command outputs *num* pseudo-random bytes after seeding the random number generator once. As in other **openssl** command line tools, PRNG seeding uses the file *\$HOME/.rnd* or *.rnd* in addition to the files given in the **-rand** option. A new *\$HOME/.rnd* or *.rnd* file will be written back if enough seeding was obtained from these sources.

**OPTIONS****-help**

Print out a usage message.

**-out** *file*

Write to *file* instead of standard output.

**-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.

**-base64**

Perform base64 encoding on the output.

**-hex**

Show the output as a hex string.

**SEE ALSO**

**RAND\_bytes**(3)

**COPYRIGHT**

Copyright 2000–2016 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>>.