

**NAME**

rand – generate pseudo-random bytes

**SYNOPSIS**

**openssl rand** [**-out** *file*] [**-rand** *file(s)*] [**-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**

**-out** *file*

Write to *file* instead of standard output.

**-rand** *file(s)*

Use specified file or files or EGD socket (see *RAND\_egd(3)*) for seeding the random number generator. Multiple files can be specified separated by a OS-dependent character. The separator is **;** for MS-Windows, **,** for OpenVMS, and **:** for all others.

**-base64**

Perform base64 encoding on the output.

**-hex**

Show the output as a hex string.

**SEE ALSO**

*RAND\_bytes(3)*