NAME

openssl−genrsa, genrsa − generate an RSA private key

SYNOPSIS

openssl genrsa [**−help**] [**−out filename**] [**−passout arg**] [**−aes128**] [**−aes192**] [**−aes256**] [**−aria128**] [**−aria192**] [**−aria256**] [**−camellia128**] [**−camellia192**] [**−camellia256**] [**−des**] [**−des3**] [**−idea**] [**−f4**] [**−3**] [**−rand file...**] [**−writerand file**] [**−engine id**] [**−primes num**] [**numbits**]

DESCRIPTION

The **genrsa** command generates an RSA private key.

OPTIONS

−help

Print out a usage message.

−out filename

Output the key to the specified file. If this argument is not specified then standard output is used.

−passout arg

The output file password source. For more information about the format of **arg** see the **PASS PHRASE ARGUMENTS** section in **openssl** (1).

−aes128, **−aes192**, **−aes256**, **−aria128**, **−aria192**, **−aria256**, **−camellia128**, **−camellia192**, **−camellia256**, **−des**, **−des3**, **−idea**

These options encrypt the private key with specified cipher before outputting it. If none of these options is specified no encryption is used. If encryption is used a pass phrase is prompted for if it is not supplied via the **−passout** argument.

−F4|−3

The public exponent to use, either 65537 or 3. The default is 65537.

−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.

−engine id

Specifying an engine (by its unique **id** string) will cause **genrsa** 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.

−primes num

Specify the number of primes to use while generating the RSA key. The **num** parameter must be a positive integer that is greater than 1 and less than 16. If **num** is greater than 2, then the generated key is called a 'multi−prime' RSA key, which is defined in RFC 8017.

numbits

The size of the private key to generate in bits. This must be the last option specified. The default is 2048 and values less than 512 are not allowed.

NOTES

RSA private key generation essentially involves the generation of two or more prime numbers. When generating a private key various symbols will be output to indicate the progress of the generation. A **.** represents each number which has passed an initial sieve test, **+** means a number has passed a single round of the Miller-Rabin primality test, ***** means the current prime starts a regenerating progress due to some failed tests. A newline means that the number has passed all the prime tests (the actual number depends on the key size).

Because key generation is a random process the time taken to generate a key may vary somewhat. But in general, more primes lead to less generation time of a key.

SEE ALSO

gendsa (1)

COPYRIGHT