NAME

openssl-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**] [**-f4**] [**-3**] [**-primes** *num*] [**-verbose**] [**-traditional**] [**-rand** *files*] [**-writerand** *file*] [**-engine** *id*] [**-provider** *name*] [**-provider-path** *path*] [**-propquery** *propq*] [**numbits**]

DESCRIPTION

This 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 see **openssl-passphrase-options**(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, **-f4**, **-3**

The public exponent to use, either 65537 or 3. The default is 65537. The **-3** option has been deprecated.

-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.

-verbose

Print extra details about the operations being performed.

-traditional
Write the key using the traditional PKCS#1 format instead of the PKCS#8 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).

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

openssl(1), **openssl-genpkey**(1), **openssl-gendsa**(1)

COPYRIGHT