

NAME

`RSA_generate_key_ex`, `RSA_generate_key` - generate RSA key pair

SYNOPSIS

```
#include <openssl/rsa.h>
```

```
int RSA_generate_key_ex(RSA *rsa, int bits, BIGNUM *e, BN_GENCB *cb);
```

Deprecated:

```
#if OPENSSL_API_COMPAT < 0x00908000L
RSA *RSA_generate_key(int num, unsigned long e,
void (*callback)(int, int, void *), void *cb_arg);
#endif
```

DESCRIPTION

`RSA_generate_key_ex()` generates a key pair and stores it in the **RSA** structure provided in **rsa**. The pseudo-random number generator must be seeded prior to calling `RSA_generate_key_ex()`.

The modulus size will be of length **bits**, and the public exponent will be **e**. Key sizes with **num** < 1024 should be considered insecure. The exponent is an odd number, typically 3, 17 or 65537.

A callback function may be used to provide feedback about the progress of the key generation. If **cb** is not **NULL**, it will be called as follows using the `BN_GENCB_call()` function described on the [BN_generate_prime\(3\)](#) page.

- While a random prime number is generated, it is called as described in [BN_generate_prime\(3\)](#).
- When the n-th randomly generated prime is rejected as not suitable for the key, `BN_GENCB_call(cb, 2, n)` is called.
- When a random p has been found with p-1 relatively prime to **e**, it is called as `BN_GENCB_call(cb, 3, 0)`.

The process is then repeated for prime q with `BN_GENCB_call(cb, 3, 1)`.

`RSA_generate_key()` is deprecated (new applications should use `RSA_generate_key_ex()` instead). `RSA_generate_key()` works in the same way as `RSA_generate_key_ex()` except it uses “old style” call backs. See [BN_generate_prime\(3\)](#) for further details.

RETURN VALUE

`RSA_generate_key_ex()` returns 1 on success or 0 on error. `RSA_generate_key()` returns the key on success or **NULL** on error.

The error codes can be obtained by [ERR_get_error\(3\)](#).

BUGS

`BN_GENCB_call(cb, 2, x)` is used with two different meanings.

`RSA_generate_key()` goes into an infinite loop for illegal input values.

SEE ALSO

[ERR_get_error\(3\)](#), [RAND_bytes\(3\)](#), [RSA_generate_key\(3\)](#), [BN_generate_prime\(3\)](#)

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>.