NAME

BN_rand, BN_pseudo_rand, BN_rand_range, BN_pseudo_rand_range - generate pseudo-random number

SYNOPSIS

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

int BN_rand(BIGNUM *rnd, int bits, int top, int bottom);

int BN_pseudo_rand(BIGNUM *rnd, int bits, int top, int bottom);

int BN_rand_range(BIGNUM *rnd, BIGNUM *range);

int BN_pseudo_rand_range(BIGNUM *rnd, BIGNUM *range);
```

DESCRIPTION

BN_rand() generates a cryptographically strong pseudo-random number of **bits** bits in length and stores it in **rnd**. If **top** is -1, the most significant bit of the random number can be zero. If **top** is 0, it is set to 1, and if **top** is 1, the two most significant bits of the number will be set to 1, so that the product of two such random numbers will always have 2***bits** length. If **bottom** is true, the number will be odd.

BN_pseudo_rand() does the same, but pseudo-random numbers generated by this function are not necessarily unpredictable. They can be used for non-cryptographic purposes and for certain purposes in cryptographic protocols, but usually not for key generation etc.

BN_rand_range() generates a cryptographically strong pseudo-random number **rnd** in the range 0 <lt>= **rnd** < **range**. *BN_pseudo_rand_range()* does the same, but is based on *BN_pseudo_rand()*, and hence numbers generated by it are not necessarily unpredictable.

The PRNG must be seeded prior to calling *BN_rand()* or *BN_rand_range()*.

RETURN VALUES

The functions return 1 on success, 0 on error. The error codes can be obtained by *ERR_get_error(3)*.

SEE ALSO

bn(3), *ERR_get_error(3)*, *rand(3)*, *RAND_add(3)*, *RAND_bytes(3)*

HISTORY

BN_rand() is available in all versions of SSLeay and OpenSSL. *BN_pseudo_r and()* was added in OpenSSL 0.9.5. The **top** == -1 case and the function *BN_rand_range()* were added in OpenSSL 0.9.6a. *BN_pseudo_rand_range()* was added in OpenSSL 0.9.6c.