Rocky Enterprise Linux 9.2 Manual Pages on command 'BN_security_bits.3ossl'

$ man BN_security_bits.3ossl

BN_SECURITY_BITS(3ossl) OpenSSL BN_SECURITY_BITS(3ossl)

NAME

BN_security_bits - returns bits of security based on given numbers

SYNOPSIS

#include <openssl/bn.h>

int BN_security_bits(int L, int N);

DESCRIPTION

BN_security_bits() returns the number of bits of security provided by a specific algorithm and a particular key size. The bits of security is defined in NIST SP800-57. Currently, BN_security_bits() support two types of asymmetric algorithms: the FFC (Finite Field Cryptography) and IFC (Integer Factorization Cryptography). For FFC, e.g., DSA and DH, both parameters L and N are used to decide the bits of security, where L is the size of the public key and N is the size of the private key.

For IFC, e.g., RSA, only L is used and it's commonly considered to be the key size (modulus).

RETURN VALUES

Number of security bits.

NOTES

ECC (Elliptic Curve Cryptography) is not covered by the BN_security_bits() function. The symmetric algorithms are not covered neither.

SEE ALSO

DH_security_bits(3), DSA_security_bits(3), RSA_security_bits(3)

HISTORY

The BN_security_bits() function was added in OpenSSL 1.1.0.

COPYRIGHT