NAME

BN_mod_inverse - compute inverse modulo n

SYNOPSIS

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

 BIGNUM *BN_mod_inverse(BIGNUM *r, BIGNUM *a, const BIGNUM *n,
                        BN_CTX *ctx);
```

DESCRIPTION

BN_mod_inverse() computes the inverse of **a** modulo **n** places the result in **r** ("(a*r)%n==1"). If **r** is NULL, a new **BIGNUM** is created.

ctx is a previously allocated **BN_CTX** used for temporary variables. **r** may be the same **BIGNUM** as **a** or **n**.

RETURN VALUES

BN_mod_inverse() returns the **BIGNUM** containing the inverse, and NULL on error. The error codes can be obtained by **ERR_get_error**(3).

SEE ALSO

ERR_get_error(3), **BN_add**(3)

COPYRIGHT