

**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**

*bn(3)*, *ERR\_get\_error(3)*, *BN\_add(3)*

**HISTORY**

*BN\_mod\_inverse()* is available in all versions of SSLeay and OpenSSL.