NAME

RSA_blinding_on, RSA_blinding_off - protect the RSA operation from timing attacks

SYNOPSIS

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

int RSA_blinding_on(RSA *rsa, BN_CTX *ctx);

void RSA_blinding_off(RSA *rsa);
```

DESCRIPTION

RSA is vulnerable to timing attacks. In a setup where attackers can measure the time of RSA decryption or signature operations, blinding must be used to protect the RSA operation from that attack.

RSA_blinding_on() turns blinding on for key **rsa** and generates a random blinding factor. **ctx** is **NULL** or a pre-allocated and initialized **BN_CTX**. The random number generator must be seeded prior to calling *RSA_blinding_on()*.

RSA_blinding_off() turns blinding off and frees the memory used for the blinding factor.

RETURN VALUES

RSA_blinding_on() returns 1 on success, and 0 if an error occurred.

RSA_blinding_off() returns no value.

COPYRIGHT