

**NAME**

RC4\_set\_key, RC4 – RC4 encryption

**SYNOPSIS**

```
#include <openssl/rc4.h>
```

```
void RC4_set_key(RC4_KEY *key, int len, const unsigned char *data);
```

```
void RC4(RC4_KEY *key, unsigned long len, const unsigned char *indata,  
         unsigned char *outdata);
```

**DESCRIPTION**

This library implements the Alleged RC4 cipher, which is described for example in *Applied Cryptography*. It is believed to be compatible with RC4[TM], a proprietary cipher of RSA Security Inc.

RC4 is a stream cipher with variable key length. Typically, 128 bit (16 byte) keys are used for strong encryption, but shorter insecure key sizes have been widely used due to export restrictions.

RC4 consists of a key setup phase and the actual encryption or decryption phase.

**RC4\_set\_key()** sets up the **RC4\_KEY** key using the **len** bytes long key at **data**.

**RC4()** encrypts or decrypts the **len** bytes of data at **indata** using **key** and places the result at **outdata**. Repeated **RC4()** calls with the same **key** yield a continuous key stream.

Since RC4 is a stream cipher (the input is XORed with a pseudo-random key stream to produce the output), decryption uses the same function calls as encryption.

**RETURN VALUES**

**RC4\_set\_key()** and **RC4()** do not return values.

**NOTE**

Applications should use the higher level functions [EVP\\_EncryptInit\(3\)](#) etc. instead of calling these functions directly.

It is difficult to securely use stream ciphers. For example, do not perform multiple encryptions using the same key stream.

**SEE ALSO**

[EVP\\_EncryptInit\(3\)](#)

**COPYRIGHT**

Copyright 2000–2016 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (the “License”). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.