NAME

EVP_rc4, EVP_rc4_40, EVP_rc4_hmac_md5 - EVP RC4 stream cipher

SYNOPSIS

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

const EVP_CIPHER *EVP_rc4(void);
const EVP_CIPHER *EVP_rc4_40(void);
const EVP_CIPHER *EVP_rc4_hmac_md5(void);
```

DESCRIPTION

The RC4 stream cipher for EVP.

EVP_rc4()

RC4 stream cipher. This is a variable key length cipher with a default key length of 128 bits.

EVP_rc4_40()

RC4 stream cipher with 40 bit key length.

WARNING: this function is obsolete. Its usage should be replaced with the **EVP_rc4()** and the **EVP_CIPHER_CTX_set_key_length()** functions.

EVP_rc4_hmac_md5()

Authenticated encryption with the RC4 stream cipher with MD5 as HMAC.

WARNING: this is not intended for usage outside of TLS and requires calling of some undocumented ctrl functions. These ciphers do not conform to the EVP AEAD interface.

NOTES

Developers should be aware of the negative performance implications of calling these functions multiple times and should consider using **EVP_CIPHER_fetch**(3) instead. See "Performance" in **crypto**(7) for further information.

RETURN VALUES

These functions return an **EVP_CIPHER** structure that contains the implementation of the symmetric cipher. See **EVP_CIPHER_meth_new**(3) for details of the **EVP_CIPHER** structure.

SEE ALSO

evp(7), **EVP_EncryptInit**(3), **EVP_CIPHER_meth_new**(3)

COPYRIGHT