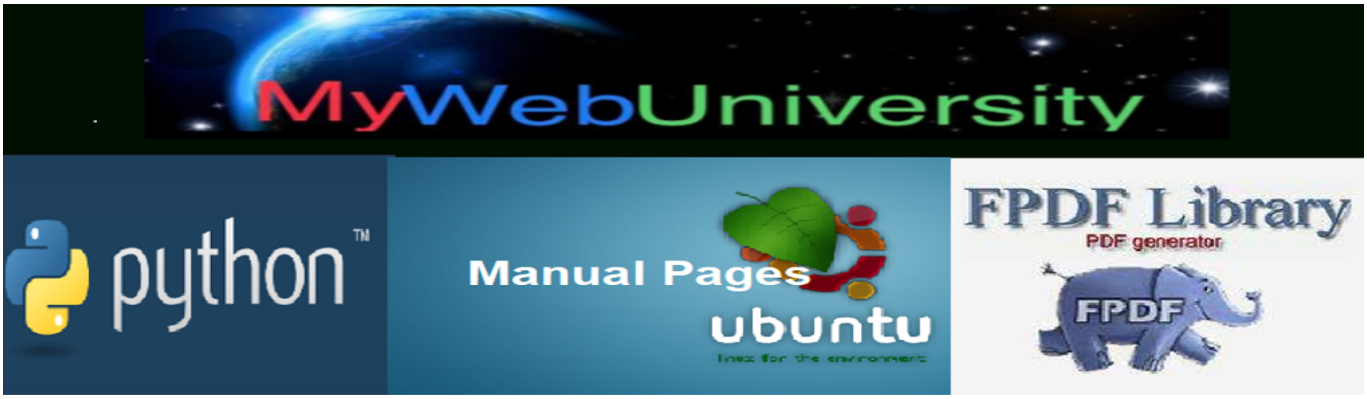

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Mac::XCBC.3pm'

$ man Crypt::Mac::XCBC.3pm

Crypt::Mac::XCBC(3pm) User Contributed Perl Documentation Crypt::Mac::XCBC(3pm)

NAME

Crypt::Mac::XCBC - Message authentication code XCBC (RFC 3566)

SYNOPSIS

```
### Functional interface:
use Crypt::Mac::XCBC qw( xcbc xcbc_hex );

# calculate MAC from string/buffer
$xcbc_raw  = xcbc($cipher_name, $key, 'data buffer');
$xcbc_hex  = xcbc_hex($cipher_name, $key, 'data buffer');
$xcbc_b64  = xcbc_b64($cipher_name, $key, 'data buffer');
$xcbc_b64u = xcbc_b64u($cipher_name, $key, 'data buffer');

### OO interface:
use Crypt::Mac::XCBC;

$d = Crypt::Mac::XCBC->new($cipher_name, $key);
$d->add('any data');
$d->addfile('filename.dat');
$d->addfile(*FILEHANDLE);
$result_raw  = $d->mac;     # raw bytes
```

```
$result_hex  = $d->hexmac;  # hexadecimal form
$result_b64  = $d->b64mac;  # Base64 form
$result_b64u = $d->b64umac; # Base64 URL Safe form
```

DESCRIPTION

Provides an interface to the XCBC message authentication code (MAC) algorithm.

EXPORT

Nothing is exported by default.

You can export selected functions:

```
use Crypt::Mac::XCBC qw(xcbc xcbc_hex );
```

Or all of them at once:

```
use Crypt::Mac::XCBC ':all';
```

FUNCTIONS

xcbc

Logically joins all arguments into a single string, and returns its XCBC message authentication code encoded as a binary string.

```
$xcbc_raw = xcbc($cipher_name, $key, 'data buffer');
#or
$xcbc_raw = xcbc($cipher_name, $key, 'any data', 'more data', 'even more data');
```

xcbc_hex

Logically joins all arguments into a single string, and returns its XCBC message authentication code encoded as a hexadecimal string.

```
$xcbc_hex = xcbc_hex($cipher_name, $key, 'data buffer');
#or
```

```
$xcbc_hex = xcbc_hex($cipher_name, $key, 'any data', 'more data', 'even more data');
```

xcbc_b64

Logically joins all arguments into a single string, and returns its XCBC message authentication code encoded as a Base64 string.

```
$xcbc_b64 = xcbc_b64($cipher_name, $key, 'data buffer');
#or
$xcbc_b64 = xcbc_b64($cipher_name, $key, 'any data', 'more data', 'even more data');
```

xcbc_b64u

Logically joins all arguments into a single string, and returns its XCBC message authentication code encoded as a Base64 URL Safe string (see RFC 4648 section 5).

```
$xcbc_b64url = xcbc_b64u($cipher_name, $key, 'data buffer');
#or
$xcbc_b64url = xcbc_b64u($cipher_name, $key, 'any data', 'more data', 'even more data');
```

METHODS

new

```
$d = Crypt::Mac::XCBC->new($cipher_name, $key);
```

clone

```
$d->clone();
```

reset

```
$d->reset();
```

add

```
$d->add('any data');
#or
$d->add('any data', 'more data', 'even more data');
```

addfile

```
$d->addfile('filename.dat');
#or
$d->addfile(*FILEHANDLE);
```

mac

```
$result_raw = $d->mac();
```

hexmac

```
$result_hex = $d->hexmac();
```

b64mac

```
$result_b64 = $d->b64mac();
```

b64umac

```
$result_b64url = $d->b64umac();
```

SEE ALSO

- CryptX
- <https://www.ietf.org/rfc/rfc3566.txt>