



Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!

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

\$ man Crypt::Mac::OMAC.3pm

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

NAME

Crypt::Mac::OMAC - Message authentication code OMAC

SYNOPSIS

Functional interface:

```
use Crypt::Mac::OMAC qw( omac omac_hex );
```

```
# calculate MAC from string/buffer
```

```
$omac_raw = omac($cipher_name, $key, 'data buffer');
```

```
$omac_hex = omac_hex($cipher_name, $key, 'data buffer');
```

```
$omac_b64 = omac_b64($cipher_name, $key, 'data buffer');
```

```
$omac_b64u = omac_b64u($cipher_name, $key, 'data buffer');
```

OO interface:

```
use Crypt::Mac::OMAC;
```

```
$d = Crypt::Mac::OMAC->new($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 OMAC message authentication code (MAC) algorithm.

EXPORT

Nothing is exported by default.

You can export selected functions:

```
use Crypt::Mac::OMAC qw(omac omac_hex );
```

Or all of them at once:

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

FUNCTIONS

omac

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

```
$omac_raw = omac($cipher_name, $key, 'data buffer');
```

#or

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

omac_hex

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

```
$omac_hex = omac_hex($cipher_name, $key, 'data buffer');
```

#or

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

omac_b64

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

```
$omac_b64 = omac_b64($cipher_name, $key, 'data buffer');
```

#or

```
$omac_b64 = omac_b64($cipher_name, $key, 'any data', 'more data', 'even more data');
```

omac_b64u

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

```
$omac_b64url = omac_b64u($cipher_name, $key, 'data buffer');
```

#or

```
$omac_b64url = omac_b64u($cipher_name, $key, 'any data', 'more data', 'even more data');
```

METHODS

new

```
$d = Crypt::Mac::OMAC->new($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://en.wikipedia.org/wiki/OMAC_%28cryptography%29>

perl v5.34.0

2022-02-06

Crypt::Mac::OMAC(3pm)