



**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::Mode::CTR.3pm'***

***\$ man Crypt::Mode::CTR.3pm***

Crypt::Mode::CTR(3pm)      User Contributed Perl Documentation      Crypt::Mode::CTR(3pm)

**NAME**

Crypt::Mode::CTR - Block cipher mode CTR [Counter mode]

**SYNOPSIS**

```
use Crypt::Mode::CTR;

my $m = Crypt::Mode::CTR->new('AES');

#(en|de)crypt at once

my $ciphertext = $m->encrypt($plaintext, $key, $iv);
my $plaintext = $m->decrypt($ciphertext, $key, $iv);

#encrypt more chunks

$m->start_encrypt($key, $iv);

my $ciphertext = $m->add('some data');
$ciphertext .= $m->add('more data');

#decrypt more chunks

$m->start_decrypt($key, $iv);

my $plaintext = $m->add($some_ciphertext);
$plaintext .= $m->add($more_ciphertext);
```

## DESCRIPTION

This module implements CTR cipher mode. NOTE: it works only with ciphers from CryptX (Crypt::Cipher::NNNN).

## METHODS

### new

```
my $m = Crypt::Mode::CTR->new($cipher_name);  
#or  
my $m = Crypt::Mode::CTR->new($cipher_name, $ctr_mode, $ctr_width);  
#or  
my $m = Crypt::Mode::CTR->new($cipher_name, $ctr_mode, $ctr_width, $cipher_rounds);  
  
# $cipher_name .. one of 'AES', 'Anubis', 'Blowfish', 'CAST5', 'Camellia', 'DES', 'DES_EDE',  
#       'KASUMI', 'Khazad', 'MULTI2', 'Noekeon', 'RC2', 'RC5', 'RC6',  
#       'SAFERP', 'SAFER_K128', 'SAFER_K64', 'SAFER_SK128', 'SAFER_SK64',  
#       'SEED', 'Skipjack', 'Twofish', 'XTEA', 'IDEA', 'Serpent'  
#       simply any <NAME> for which there exists Crypt::Cipher::<NAME>  
# $ctr_mode ..... 0 little-endian counter (DEFAULT)  
#       1 big-endian counter  
#       2 little-endian + RFC3686 incrementing  
#       3 big-endian + RFC3686 incrementing  
# $ctr_width .... counter width in bytes (DEFAULT = full block width)  
# $cipher_rounds ... optional num of rounds for given cipher
```

### encrypt

```
my $ciphertext = $m->encrypt($plaintext, $key, $iv);
```

### decrypt

```
my $plaintext = $m->decrypt($ciphertext, $key, $iv);
```

### start\_encrypt

```
$m->start_encrypt($key, $iv);
```

start\_decrypt

```
$m->start_decrypt($key, $iv);
```

add

```
# in encrypt mode
```

```
my $plaintext = $m->add($ciphertext);
```

```
# in decrypt mode
```

```
my $ciphertext = $m->add($plaintext);
```

SEE ALSO

? CryptX, Crypt::Cipher

? Crypt::Cipher::AES, Crypt::Cipher::Blowfish, ...

? <[https://en.wikipedia.org/wiki/Block\\_cipher\\_mode\\_of\\_operation#Counter\\_.28CTR.29](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Counter_.28CTR.29)>

perl v5.34.0

2022-02-06

Crypt::Mode::CTR(3pm)