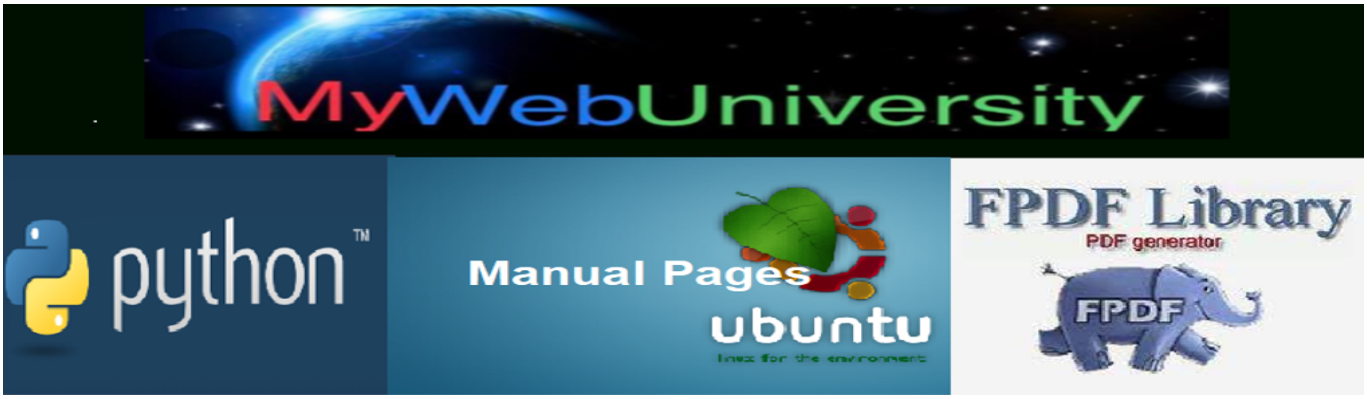

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Stream::ChaCha.3pm'

$ man Crypt::Stream::ChaCha.3pm

Crypt::Stream::ChaCha(3pm) User Contributed Perl Documentation Crypt::Stream::ChaCha(3pm)

NAME

Crypt::Stream::ChaCha - Stream cipher ChaCha

SYNOPSIS

```
use Crypt::Stream::ChaCha;

# encrypt

$key = "1234567890123456";

$iv  = "123456789012";

$stream = Crypt::Stream::ChaCha->new($key, $iv);

$ct = $stream->crypt("plain message");

# decrypt

$key = "1234567890123456";

$iv  = "123456789012";

$stream = Crypt::Stream::ChaCha->new($key, $iv);

$pt = $stream->crypt($ct);
```

DESCRIPTION

Provides an interface to the ChaCha stream cipher.

METHODS

new

```
$stream = Crypt::Stream::ChaCha->new($key, $iv);

#or

$stream = Crypt::Stream::ChaCha->new($key, $iv, $counter, $rounds);

# $key     .. 32 or 16 bytes
```

```
    # $iv      .. 8 or 12 bytes
    # $counter .. initial counter value (DEFAULT: 0)
    # $rounds  .. rounds (DEFAULT: 20)
  crypt
    $ciphertext = $stream->crypt($plaintext);
    #or
    $plaintext = $stream->crypt($ciphertext);
  keystream
    $random_key = $stream->keystream($length);
  clone
    $stream->clone();
SEE ALSO
    ?  Crypt::Stream::RC4, Crypt::Stream::Sober128, Crypt::Stream::Salsa20,
       Crypt::Stream::Sosemanuk
    ?  <https://tools.ietf.org/html/rfc7539>
perl v5.34.0                    2022-02-06              Crypt::Stream::ChaCha(3pm)
```