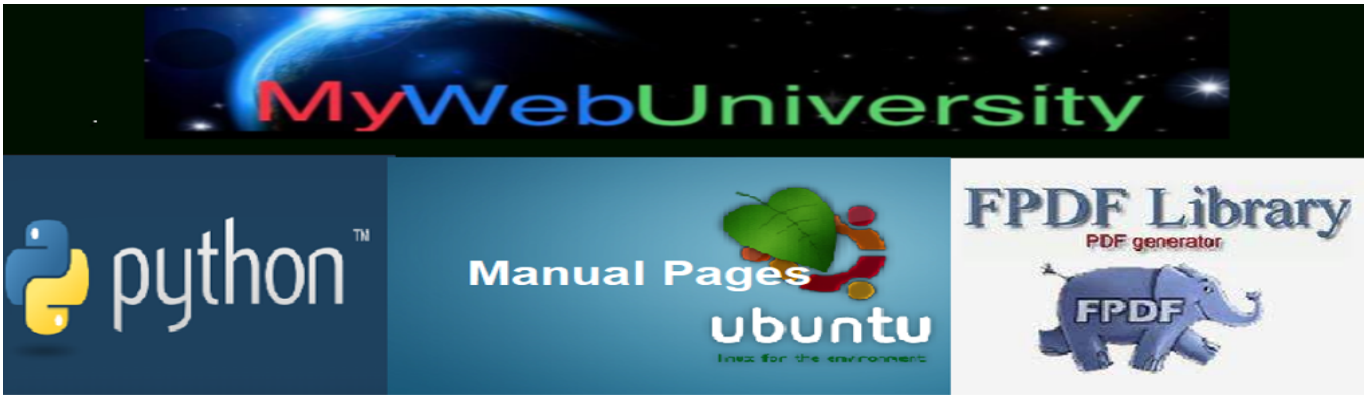

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Stream::Salsa20.3pm'

$ man Crypt::Stream::Salsa20.3pm

Crypt::Stream::Salsa20(3pm) User Contributed Perl Documentation Crypt::Stream::Salsa20(3pm)

NAME

Crypt::Stream::Salsa20 - Stream cipher Salsa20

SYNOPSIS

```
use Crypt::Stream::Salsa20;
# encrypt
$key = "1234567890123456";
$iv  = "12345678";
$stream = Crypt::Stream::Salsa20->new($key, $iv);
$ct = $stream->crypt("plain message");
# decrypt
$key = "1234567890123456";
$iv  = "12345678";
$stream = Crypt::Stream::Salsa20->new($key, $iv);
$pt = $stream->crypt($ct);
```

DESCRIPTION

Provides an interface to the Salsa20 stream cipher.

METHODS

new

```
$stream = Crypt::Stream::Salsa20->new($key, $iv);
#or
$stream = Crypt::Stream::Salsa20->new($key, $iv, $counter, $rounds);
# $key     .. 32 or 16 bytes
```

```
    # $iv      .. 8 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::ChaCha, Crypt::Stream::RC4, Crypt::Stream::Sober128, Crypt::Stream::Sosemanuk