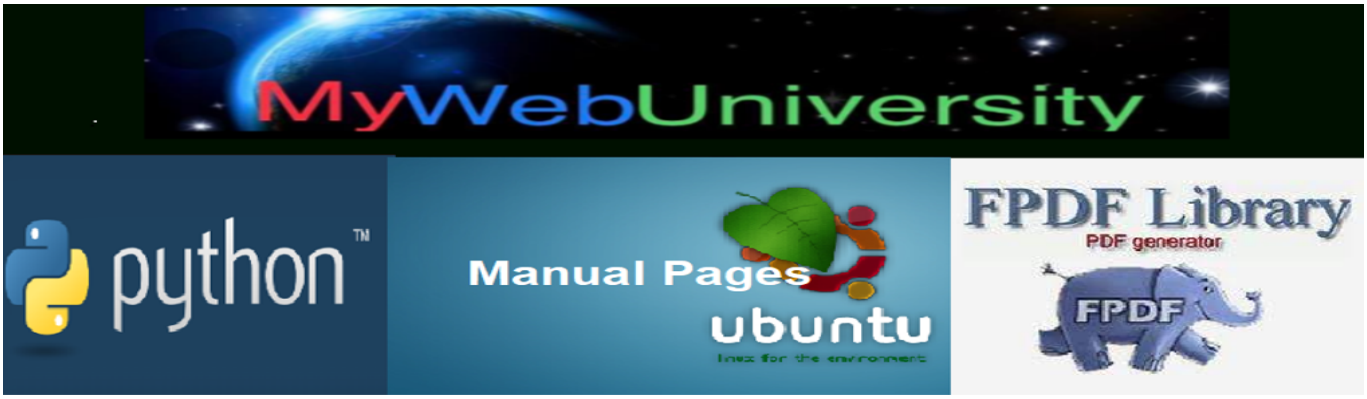

Rocky Enterprise Linux 9.2 Manual Pages on command 'Crypt::Stream::Sosemanuk.3pm'

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

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

NAME

Crypt::Stream::Sosemanuk - Stream cipher Sosemanuk

SYNOPSIS

```
use Crypt::Stream::Sosemanuk;
# encrypt
$key = "1234567890123456";
$iv  = "123456789012";
$stream = Crypt::Stream::Sosemanuk->new($key, $iv);
$ct = $stream->crypt("plain message");
# decrypt
$key = "1234567890123456";
$iv  = "123456789012";
$stream = Crypt::Stream::Sosemanuk->new($key, $iv);
$pt = $stream->crypt($ct);
```

DESCRIPTION

Provides an interface to the Sosemanuk stream cipher.

METHODS

new

```
$stream = Crypt::Stream::Sosemanuk->new($key, $iv);
# $key .. keylen must be multiple of 4 bytes
# $iv  .. ivlen must be multiple of 4 bytes (OPTIONAL)
```

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::ChaCha, Crypt::Stream::Salsa20, Crypt::Stream::Sober128
- <https://en.wikipedia.org/wiki/SOSEMANUK>