



**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::Stream::Sober128.3pm'***

***\$ man Crypt::Stream::Sober128.3pm***

Crypt::Stream::Sober128(3pm) User Contributed Perl Documentation Crypt::Stream::Sober128(3pm)

NAME

Crypt::Stream::Sober128 - Stream cipher Sober128

SYNOPSIS

```
use Crypt::Stream::Sober128;

# encrypt

$key = "1234567890123456";

$iv = "123456789012";

$stream = Crypt::Stream::Sober128->new($key, $iv);

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

# decrypt

$key = "1234567890123456";

$iv = "123456789012";

$stream = Crypt::Stream::Sober128->new($key, $iv);

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

DESCRIPTION

Provides an interface to the Sober128 stream cipher.

METHODS

new

```
$stream = Crypt::Stream::Sober128->new($key, $iv);
```

```
# $key .. keylen must be multiple of 4 bytes
```

```
# $iv .. ivlen must be multiple of 4 bytes
```

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::Sosemanuk

? <<https://en.wikipedia.org/wiki/SOBER-128>>

perl v5.34.0

2022-02-06

Crypt::Stream::Sober128(3pm)