



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::Rabbit.3pm'

\$ man Crypt::Stream::Rabbit.3pm

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

NAME

Crypt::Stream::Rabbit - Stream cipher Rabbit

SYNOPSIS

```
use Crypt::Stream::Rabbit;

# encrypt

$key = "1234567890123456";
$iv = "12345678";
$stream = Crypt::Stream::Rabbit->new($key, $iv);
$ct = $stream->crypt("plain message");

# decrypt

$key = "1234567890123456";
$iv = "12345678";
$stream = Crypt::Stream::Rabbit->new($key, $iv);
$pt = $stream->crypt($ct);
```

DESCRIPTION

Provides an interface to the Rabbit stream cipher.

METHODS

new

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

```
# $key .. keylen must be up to 16 bytes
```

```
# $iv .. ivlen must be up to 8 bytes
```

```
$stream = Crypt::Stream::Rabbit->new($key);
```

```
#BEWARE: this is different from new($key, "")
```

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/Rabbit_\(cipher\)](https://en.wikipedia.org/wiki/Rabbit_(cipher))>