



**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::PRNG::ChaCha20.3pm'***

***\$ man Crypt::PRNG::ChaCha20.3pm***

Crypt::PRNG::ChaCha20(3pm) User Contributed Perl Documentation Crypt::PRNG::ChaCha20(3pm)

**NAME**

Crypt::PRNG::ChaCha20 - Cryptographically secure PRNG based on ChaCha20 (stream cipher) algorithm

**SYNOPSIS**

```
### Functional interface:

    use Crypt::PRNG::ChaCha20 qw(random_bytes random_bytes_hex random_bytes_b64 random_string
random_string_from rand irand);

    $octets = random_bytes(45);
    $hex_string = random_bytes_hex(45);
    $base64_string = random_bytes_b64(45);
    $base64url_string = random_bytes_b64u(45);
    $alphanumeric_string = random_string(30);
    $string = random_string_from('ACGT', 64);
    $floating_point_number_0_to_1 = rand;
    $floating_point_number_0_to_88 = rand(88);
    $unsigned_32bit_int = irand;

### OO interface:

use Crypt::PRNG::ChaCha20;
```

```
$prng = Crypt::PRNG::ChaCha20->new;
#or
$prng = Crypt::PRNG::ChaCha20->new("some data used for seeding PRNG");

$octets = $prng->bytes(45);
$hex_string = $prng->bytes_hex(45);
$base64_string = $prng->bytes_b64(45);
$base64url_string = $prng->bytes_b64u(45);
$alphanumeric_string = $prng->string(30);
$string = $prng->string_from('ACGT', 64);
$floating_point_number_0_to_1 = rand;
$floating_point_number_0_to_88 = rand(88);
$unsigned_32bit_int = irand;
```

## DESCRIPTION

Provides an interface to the ChaCha20 based pseudo random number generator

All methods and functions are the same as for Crypt::PRNG.

## FUNCTIONS

random\_bytes

See "random\_bytes" in Crypt::PRNG.

random\_bytes\_hex

See "random\_bytes\_hex" in Crypt::PRNG.

random\_bytes\_b64

See "random\_bytes\_b64" in Crypt::PRNG.

random\_bytes\_b64u

See "random\_bytes\_b64u" in Crypt::PRNG.

random\_string

See "random\_string" in Crypt::PRNG.

random\_string\_from

See "random\_string\_from" in Crypt::PRNG.

rand

See "rand" in Crypt::PRNG.

irand

See "irand" in Crypt::PRNG.

## METHODS

new

See "new" in Crypt::PRNG.

bytes

See "bytes" in Crypt::PRNG.

bytes\_hex

See "bytes\_hex" in Crypt::PRNG.

bytes\_b64

See "bytes\_b64" in Crypt::PRNG.

bytes\_b64u

See "bytes\_b64u" in Crypt::PRNG.

string

See "string" in Crypt::PRNG.

string\_from

See "string\_from" in Crypt::PRNG.

double

See "double" in Crypt::PRNG.

int32

See "int32" in Crypt::PRNG.

#### SEE ALSO

? Crypt::PRNG

? <<https://tools.ietf.org/html/rfc7539>>

perl v5.34.0

2022-02-06

Crypt::PRNG::ChaCha20(3pm)