



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::Yarrow.3pm'

\$ man Crypt::PRNG::Yarrow.3pm

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

NAME

Crypt::PRNG::Yarrow - Cryptographically secure PRNG based on Yarrow algorithm

SYNOPSIS

Functional interface:

```
use Crypt::PRNG::Yarrow 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::Yarrow;
```

```
$prng = Crypt::PRNG::Yarrow->new;

#or

$prng = Crypt::PRNG::Yarrow->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 Yarrow 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://en.wikipedia.org/wiki/Yarrow_algorithm>

perl v5.34.0

2022-02-06

Crypt::PRNG::Yarrow(3pm)