

Module sui::random

This module provides functionality for generating secure randomness.

Singleton shared object which stores the global randomness state. The actual state is stored in a versioned inner field.

Unique randomness generator, derived from the global randomness.

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be called by genesis or change_epoch transactions.

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

Create a generator. Can be used to derive up to $\text{MAX_U16} * 32$ random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see: <https://docs.sui.io/guides/developer/advanced/randomness-onchain>

Get the next block of 32 random bytes.

Generate n random bytes.

Generate a u256.

Generate a u128.

Generate a u64.

Generate a u32.

Generate a u16.

Generate a u8.

Generate a boolean.

Helper macro to generate a random uint in [min, max] using a random number with num_of_bytes bytes. Assumes that the caller verified the inputs, and uses num_of_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

Generate a random u128 in [min, max] (with a bias of $2^{\{-64\}}$).

Generate a random u32 in [min, max] (with a bias of $2^{\{-64\}}$).

Generate a random u16 in [min, max] (with a bias of $2^{\{-64\}}$).

Generate a random u8 in [min, max] (with a bias of $2^{\{-64\}}$).

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

Struct

Singleton shared object which stores the global randomness state. The actual state is stored in a versioned inner field.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Unique randomness generator, derived from the global randomness.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be called by genesis or change_epoch transactions.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create a generator. Can be used to derive up to $\text{MAX_U16} * 32$ random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Get the next block of 32 random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate n random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u256.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u128.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u64.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u32.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in $[\text{min}, \text{max}]$ using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Struct

```
'''bash
```

```
'''
```

Unique randomness generator, derived from the global randomness.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be called by genesis or change\_epoch transactions.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see: <https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
'''
```

Generate a u32.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u16.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u8.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a boolean.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Helper macro to generate a random uint in [min, max] using a random number with num_of_bytes bytes. Assumes that the caller verified the inputs, and uses num_of_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in [min, max] (with a bias of $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```



```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of 2^{-64}).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of 2^{-64}).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of 2^{-64}).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Struct

Unique randomness generator, derived from the global randomness.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be called by genesis or change_epoch transactions.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Create a generator. Can be used to derive up to MAX_U16 * 32 random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see: <https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in [min, max] using a random number with num_of_bytes bytes. Assumes that the caller verified the inputs, and uses num_of_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of 2^{-64}).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of 2^{-64}).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Constants

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be

called by genesis or change_epoch transactions.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Create a generator. Can be used to derive up to $\text{MAX_U16} * 32$ random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

'''

'''bash

'''

'''bash

'''

Generate a u256.

'''bash

'''

'''bash

'''

Generate a u128.

'''bash

'''

'''bash

'''

Generate a u64.

'''bash

'''

'''bash

'''

Generate a u32.

'''bash

'''

'''bash

'''

Generate a u16.

'''bash

'''

'''bash

'''

Generate a u8.

'''bash

'''

'''bash

```
'''
```

Generate a boolean.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```



```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

## Function

Create and share the Random object. This function is called exactly once, when the Random object is first created. Can only be called by genesis or change\_epoch transactions.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in  $[\text{min}, \text{max}]$  using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Function

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Get the next block of 32 random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate n random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u256.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u128.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u64.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u8.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a boolean.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Function

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.



```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u8.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a boolean.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Function

Record new randomness. Called when executing the RandomnessStateUpdate system transaction.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Function

Create a generator. Can be used to derive up to  $\text{MAX\_U16} * 32$  random bytes.

Using randomness can be error-prone if you don't observe the subtleties in its correct use, for example, randomness dependent code might be exploitable to attacks that carefully set the gas budget in a way that breaks security. For more information, see:

<https://docs.sui.io/guides/developer/advanced/randomness-onchain>

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Get the next block of 32 random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate n random bytes.

```
'''bash
```

```
'''
```

```
'''bash
```

'''

'''bash

'''

'''bash

'''

Generate a u256.

'''bash

'''

'''bash

'''

Generate a u128.

'''bash

'''

'''bash

'''

Generate a u64.

'''bash

'''

'''bash

'''

Generate a u32.

'''bash

'''

'''bash

'''

Generate a u16.

'''bash

'''

'''bash

'''

Generate a u8.

'''bash

'''

'''bash

```
'''
```

Generate a boolean.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

## Function

Get the next block of 32 random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```



```
...
```

```
```bash
```

```
...
```

Generate a u32.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in  $[\text{min}, \text{max}]$  using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

## Function

Generate n random bytes.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u8.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a boolean.

```
```bash
```

```
```
```

```
```bash
```

```
'''
```

Helper macro to generate a random uint in [min, max] using a random number with num_of_bytes bytes. Assumes that the caller verified the inputs, and uses num_of_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in [min, max] (with a bias of $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of $2^{\{-64\}}$).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
```bash
```

```
```
```

Macro function

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in $[\text{min}, \text{max}]$ using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Function

Generate a u256.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u128.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u16.

```
```bash
```

```
```
```

```
```bash
```

```
'''
```

Generate a u8.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a boolean.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Helper macro to generate a random uint in `[min, max]` using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```



```
```bash
```

```
```
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

## Function

Generate a ul28.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u64.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u32.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a ul6.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a u8.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a boolean.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Helper macro to generate a random uint in  $[\text{min}, \text{max}]$  using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u128 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u16 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Function

Generate a u64.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u32.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u16.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a u8.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
```
```

Helper macro to generate a random uint in [min, max] using a random number with num_of_bytes bytes. Assumes that the caller verified the inputs, and uses num_of_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u128 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u16 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u8 in [min, max] (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Function

Generate a u32.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u16.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u8.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a boolean.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Helper macro to generate a random uint in  $[\text{min}, \text{max}]$  using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in  $[\text{min}, \text{max}]$  (with a bias of  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Function

Generate a u16.

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a u8.

```
'''bash
```

```
...
```

```
```bash
```

```
...
```

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in $[\text{min}, \text{max}]$ using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Function

Generate a u8.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a boolean.

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Helper macro to generate a random uint in $[\text{min}, \text{max}]$ using a random number with `num_of_bytes` bytes. Assumes that the caller verified the inputs, and uses `num_of_bytes` to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random ul28 in $[\text{min}, \text{max}]$ (with a bias of $2^{\{-64\}}$).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```



```
```bash
```

```
...
```

Generate a random u32 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Function

Generate a boolean.

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u128 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u32 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Macro function

Helper macro to generate a random uint in [min, max] using a random number with num\_of\_bytes bytes. Assumes that the caller verified the inputs, and uses num\_of\_bytes to control the bias (e.g., 8 bytes larger than the actual type used by the caller function to limit the bias by  $2^{\{-64\}}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u128 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```

## Function

Generate a random `u128` in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random `u32` in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random `u16` in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random `u8` in `[min, max]` (with a bias of  $2^{\{-64\}}$ ).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

## Function

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

## Function

Generate a random u32 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u16 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
...
```

Generate a random u8 in [min, max] (with a bias of  $2^{-64}$ ).

```
```bash
```

```
...
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Function

Generate a random u16 in [min, max] (with a bias of 2^{-64}).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Generate a random u8 in [min, max] (with a bias of 2^{-64}).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Function

Generate a random u8 in [min, max] (with a bias of 2^{-64}).

```
```bash
```

```
```
```

```
```bash
```

```
```
```

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
```bash
```

```
```
```

```
```bash
```

```
'''
```

## Function

Shuffle a vector using the random generator (Fisher–Yates/Knuth shuffle).

```
'''bash
```

```
'''
```

```
'''bash
```

```
'''
```