

Roll your own seed phrase.

A short summary how to convert physical dice rolls into a 12- or 24-word BIP-39 seed phrase.

You can use this printed guide for a real seed phrase. If you encounter difficulties in the process, feel free to go back to the online guide and make a dry run with a dummy phrase. Keep rolls, bits, and seed words for your real seed phrase off networked devices.

Prepare

Dice

Plain, well-made six-sided dice.
Avoid decorative, novelty, damaged, or visibly uneven dice.

Rolling setup

A lidded box with enough room for every die to move freely, or a large cup and hard rolling tray.

Printouts

One Bit-to-word worksheet and the searchable BIP-39 word list.

Pen

To write bits/words on paper.
Never type those into a connected device.

Offline checksum device

A hardware wallet or permanently offline laptop that supports checksum completion.

Private room

No cameras, phones, smart glasses, observers, or recording devices.

1

Choose one encoding

Oren's variable-length mapping — recommended

- 1 → 00
- 2 → 01
- 3 → 10
- 4 → 11
- 5 → 0
- 6 → 1

Expect about 77 rolls for 12 words, or 154 for 24 words.

Binary quantization

- 1, 2, or 3 → 0
- 4, 5, or 6 → 1

You will make exactly 128 rolls for 12 words, or 256 for 24 words.

2

Choose your phrase length

Choose either 12 or 24 words.

Print the matching BitsToWord worksheet and write an **arbitrary identifier** on it so you can recognize the backup later.

3

Roll and record

Lidded box: Put all dice in the box, close the lid, and shake vigorously at least ten times. Each shake should make the dice travel and collide audibly inside. Put the box down, gently tip the settled dice to one edge, then read left to right (and front to back for another row). Do not arrange dice by hand.

Cup and tray: Shake vigorously, cast with enough room and energy for several impacts, and read dice by a spatial rule chosen before the first throw.

Convert every result with the encoding you chose and write the bits into the next empty boxes. If any die is cocked or ambiguous, discard the **whole batch** and roll that complete batch again.

Repeat until you reach the bold divider in the final word. Leave the final 4 boxes blank for a 12-word phrase, or the final 8 boxes blank for a 24-word phrase. Discard bits that would cross this boundary, then ignore all later dice in the batch.

4

Convert bits to words

For each completed 11-bit group, use the printed BIP-39 word list to find the corresponding word:

- bits 1–3 select the **page**;
- bits 4–6 select the **column**;
- bits 7–11 select the **row** and therefore the word.

Write the word beneath its 11 bits. Do not search the word list digitally, even for a partial bit pattern.

5

Complete the final word

The final word has checksum bits that are fully determined by the bits already recorded. They do not reduce the randomness supplied by the dice.

- For 12 words, your seven rolled final-word bits leave **16** possible words.
- For 24 words, your three rolled final-word bits leave **256** possible words.

Enter the earlier words as an existing seed phrase into your hardware wallet/off-line computer. Let it propose a final word, then verify that the proposed word is within the range of possible words.

Keep your seed phrase private, offline, and backed up safely.