



Dice Log – Roll your own seed

SeedSigner dice mode · 24 words from 99 rolls (SHA-256) · Self-Experiment 1b

⚠ **This string of digits IS the seed.** Anyone who knows the 99 numbers can recompute the 24 words. Never photograph it, never scan it, never type it into anything digital (the one exception: the offline check below). After the check, destroy this sheet – or store it like the backup itself.

⚠ **For self-experiments:** A documented seed counts as compromised and is never used for real coins.

METHOD (SHORT VERSION – SAME THROWING TECHNIQUE AS SHEET 1A)

You need: 5 casino dice · dice cup with lid · pen · SeedSigner (dice mode, 24 words = 99 rolls). No coin, no word table.

- Throw all 5 dice together. **Every number from 1 to 6 counts** – there are no rerolls on 5/6 here.
- Fix a reading convention beforehand and keep to it: left to right, as the dice lie (top to bottom if in doubt). Do not sort them, do not move them.
- Boot the SeedSigner, **then pull the microSD** (it runs from RAM, the device says so itself). Write the 5 digits into the row and enter them on the device right away.
- 19 rounds with 5 dice, round 20 with 4 dice = **99 digits**. The SeedSigner then shows the 24 words.

1 **2** **3** **4** **5** = 5 digits per round · round 20 only 4 dice

Round	D1	D2	D3	D4	D5	Digits	Round	D1	D2	D3	D4	D5	Digits
1						5	11						55
2						10	12						60
3						15	13						65
4						20	14						70
5						25	15						75
6						30	16						80
7						35	17						85
8						40	18						90
9						45	19						95
10						50	20					×	99

The 24 words: The SeedSigner shows them on the display after the 99th digit. **They do NOT go on this sheet** – copy them by hand straight onto the backup card. This sheet carries only the digits, and those are enough to recompute the words.

TIME

Start: _____

End: _____

Typos
corrected: _____

NOTES / FAILED ATTEMPTS (FOR THE LOGBOOK)

VERIFICATION – WITHOUT THESE STEPS THE SEED IS WORTH NOTHING

- ☐ **Recompute it independently (offline computer, never online):** enter the digits into tools/mnemonic.py from the SeedSigner repo – or into the locally saved Ian Coleman tool, where you pick "**Base 10**" and set "**Mnemonic Length**" to 24 Words. ⚠ NEVER its "Dice" mode – it turns every 6 into a 0 and quietly returns a different seed.
- ☐ All 24 words match the SeedSigner display exactly. Same rolls = same seed – if one word differs, there is a typo: stop and roll again.
- ☐ Words copied by hand onto the backup card (no photo, no text file).
- ☐ This sheet destroyed – or from now on stored like the backup itself.