Playing Cards as Seed Phrase Entropy

November 16, 2026 · Document #430 · bip39-phrase.com



Photo by Grianghraf on Unsplash

A 52-card deck has about 225.6 bits of maximum entropy; learn the limits, shuffle considerations, and offline recording requirements.

Contents

How Much Entropy Is in a Deck? 1

Why Riffle Shuffles Matter 2

Recording the Order Offline 2

Limits and Safer Practice 3

FAQ 3

Sources 3

BIP39 format examples 4

Reading a BIP39 phrase 5

See also 5

A 52-card deck can represent about 225.6 bits of information when every possible card order is equally likely. That is enough raw entropy for a BIP39 12-word phrase, which encodes 128 bits of entropy plus a checksum, provided the conversion handles bias correctly. It is not enough for the 256 bits of entropy in a 24-word phrase. The limitation is mathematical: shuffling cannot create more possible final deck orders than the deck has permutations.

How Much Entropy Is in a Deck?

A deck has 52! possible orders, where 52! means multiplying every integer from 1 through 52. The information content of choosing uniformly among those orders is log2(52!), approximately 225.58 bits. This is the theoretical maximum, and it assumes every order is equally likely.

BIP39 does not turn a deck order directly into a phrase. A 12-word phrase encodes 128 bits of entropy and adds a 4-bit checksum. A 24-word phrase encodes 256 bits and adds an 8-bit checksum. The checksum helps detect errors; it does not add secret entropy, and some incorrect phrases still pass it. Consequently, one deck can provide enough theoretical entropy for a 12-word phrase, but cannot provide the full entropy of a 24-word phrase. Do not describe a 24-word phrase derived solely from one deck order as having 256 bits of entropy.

These figures describe ideal randomness, not the quality of a particular shuffle. If a person tends to leave cards in familiar patterns, or uses a predictable shuffle, the actual uncertainty can be much lower. The deck need not start in a secret order: sufficiently random shuffling can randomize a known starting order. What matters is how unpredictable the final order is to someone who might attack the wallet.

Why Riffle Shuffles Matter

A riffle shuffle splits the deck into two packets and interleaves them. Mathematical analysis of the standard riffle-shuffle model shows a sharp improvement in mixing around seven shuffles for a 52-card deck. However, after seven shuffles the total variation distance from uniform is still about 0.334 under that model, so this benchmark does not establish cryptographic-quality randomness. Fewer shuffles often leave detectable structure from the starting order.

Seven is a mixing benchmark, not a guarantee that a real person's shuffle is uniform or cryptographically secure. Real shuffles can depart from the model: packets may interleave in large clumps, parts of the deck may remain undisturbed, and repeated techniques can produce predictable results. Overhand shuffles are generally less effective at mixing than riffles. Several genuine riffle shuffles with varied cuts and interleaving can improve mixing, but no precise count by itself proves randomness.

If the deck is new or ordered, account for that known starting state. The goal is not merely to produce an order that looks mixed, but to make the final order difficult to predict. Do not let another person observe the cards or track the shuffle if they should not know the wallet's secret.

Recording the Order Offline

Record the final order on paper, privately and away from cameras, networked devices, and voice assistants. Choose one fixed direction, such as top to bottom, and one fixed way to name each card. For example, record rank and suit for every card, including the suit rather than just the rank. A 52-card record should contain each card exactly once. Keep the record legible and check it for omissions, duplicates, and transposed entries before putting the deck away.

A card order is not itself a BIP39 seed phrase. To turn it into one, a defined conversion must map the permutation to binary entropy and then apply the BIP39 process, including checksum calculation and word-list indexing. Use an audited, trusted implementation that can run fully offline, and verify its behavior before relying on it. Do not enter the recorded order into a website, online randomizer, chat, or connected wallet. Do not invent a card-to-word mapping: arbitrary mappings can be biased, omit outcomes, or produce invalid checksums.

A conversion must also handle the fact that 52! is not a power of two. One sound method assigns each permutation a unique integer from zero through 52! minus one, accepts only a range whose size is a multiple of the desired number of outputs, and maps accepted values to those outputs equally. Rejection requires a fresh, independently randomized deck order, not repeated processing of the same order. This produces unbiased bits

only if the input orders are uniform. Simply taking selected bits from a hand-designed card encoding can introduce bias. For a 12-word phrase, the conversion must supply 128 bits of entropy before the BIP39 checksum is added. Document the method so the recorded cards can be restored without guessing the procedure.

After generating the phrase offline, verify it by restoring it in the intended wallet or a compatible offline recovery tool, and confirm that it derives the expected wallet accounts and receiving addresses. Include any BIP39 passphrase and the wallet's derivation settings in your recovery planning. Keep the phrase and any card-order record protected like private keys: anyone who obtains enough information to reconstruct the phrase and any required passphrase may control the funds. Avoid storing both the cards and phrase together. Consider whether a standard hardware-wallet entropy process is more appropriate if you need a 24-word phrase with 256 bits of entropy.

Limits and Safer Practice

A deck is a physical randomness source, not a standardized seed-generation protocol. Its usefulness depends on the shuffle, the secrecy of the process, and the correctness of the conversion. Human-generated randomness can be uneven, and handling errors can make recovery impossible. For significant funds, use a reputable wallet's documented entropy-generation procedure and verify the backup by recovery testing. If using cards, document the exact offline conversion method and do not claim more entropy than the recorded deck order can provide.

FAQ

Can one deck make a 24-word BIP39 phrase with full strength?

No, not from a single final deck order alone. A uniformly random order of 52 cards contains about 225.6 bits, below the 256 bits required for full 24-word entropy. A conversion can produce a valid 24-word phrase, but it cannot create the missing entropy.

Are seven riffle shuffles enough to guarantee randomness?

No. Seven is an approximate mixing benchmark under a mathematical shuffle model, not a cryptographic security threshold. Real shuffle technique and starting conditions affect the result.

Can I write down the cards and convert them later?

Yes, if you securely preserve the complete order and the exact documented offline conversion procedure. If that procedure rejects the order, you will need fresh randomness. A card order alone is not a BIP39 phrase.

Sources

- BIP 39: Mnemonic code for generating deterministic keys (github.com)
- Trailing the dovetail shuffle to its lair (doi.org)
- RFC 4086: Randomness Requirements for Security (www.rfc-editor.org)

> Continue reading on bip39-phrase.com: Generate a BIP39 Seed Phrase in Python: Code and Test Vectors
> More on this topic: Seed Phrases

BIP39 format examples

Randomly generated sequences of words from the BIP39 English wordlist. None of them passes the BIP39 checksum, so no wallet will accept them: they show the format only. Never store funds with a phrase you found in a document.

Example 1

1 giggle	2 nasty	3 ritual	4 luggage
5 bird	6 pond	7 fire	8 reason
9 occur	10 nurse	11 limit	12 door

Example 2

1 defense	2 jump	3 walnut	4 coin
5 oblige	6 fatal	7 tiny	8 album
9 gain	10 surround	11 tunnel	12 glove

Example 3

1 live	2 size	3 soap	4 hard
5 final	6 hurry	7 crystal	8 oxygen
9 zero	10 lunch	11 latin	12 stumble

Example 4

1 bean	2 kiwi	3 hundred	4 video
5 wild	6 insect	7 diagram	8 brick
9 admit	10 stage	11 acquire	12 identify

Example 5

1 refuse	2 blush	3 insane	4 reject
5 anxiety	6 grant	7 fly	8 junk
9 peasant	10 feed	11 sight	12 winter

Example 6

1 daughter	2 leaf	3 island	4 clown
5 asthma	6 odor	7 laundry	8 donor
9 shove	10 flush	11 spell	12 orchard

Example 7

1 room	2 hungry	3 pattern	4 collect
5 expect	6 tissue	7 outside	8 sign
9 destroy	10 walnut	11 vanish	12 siren

Example 8			
1 elder	2 goose	3 pizza	4 burst
5 viable	6 green	7 file	8 indicate
9 vacant	10 struggle	11 plate	12 beyond

Reading a BIP39 phrase

Every word stands for an 11-bit number: its position in the 2048-word list, counted from 0. Here is Example 1 decoded word by word. Each word links to its page on bip39-phrase.com, where the list is numbered from 1.

#	Word	Index (0-2047)	Word no.	11 bits
1	giggle	783	784	01100001111
2	nasty	1177	1178	10010011001
3	ritual	1492	1493	10111010100
4	luggage	1062	1063	10000100110
5	bird	180	181	00010110100
6	pond	1342	1343	10100111110
7	fire	697	698	01010111001
8	reason	1432	1433	10110011000
9	occur	1222	1223	10011000110
10	nurse	1212	1213	10010111100
11	limit	1039	1040	10000001111
12	door	523	524	01000001011

The 12 words carry 132 bits: 128 bits of entropy followed by a 4-bit checksum. The checksum must equal the first 4 bits of the SHA-256 hash of the entropy.

`Entropy (hex): 61f266ea4261694f95cd9898d2f207a0`

This sequence ends in the checksum bits 1011, but SHA-256 of its entropy starts with 0011, so wallets reject it as an invalid phrase. That is the point of the checksum: about 15 of every 16 random or mistyped sequences fail it.

See also

- Seed Access If You and Your Partner Die Together · November 15, 2026
- Why Song Lyrics and Famous Quotes Make Weak Passphrases · November 14, 2026
- Seed Phrase Planning for Incapacity and Recovery · November 13, 2026
- Asking a Chatbot for a Seed Phrase: Why It Fails · November 12, 2026

Educational document. The example sequences are random and fail the BIP39 checksum: they are not wallets and must never hold funds. Security notes: bip39-phrase.com/security/