

CORONA POKER

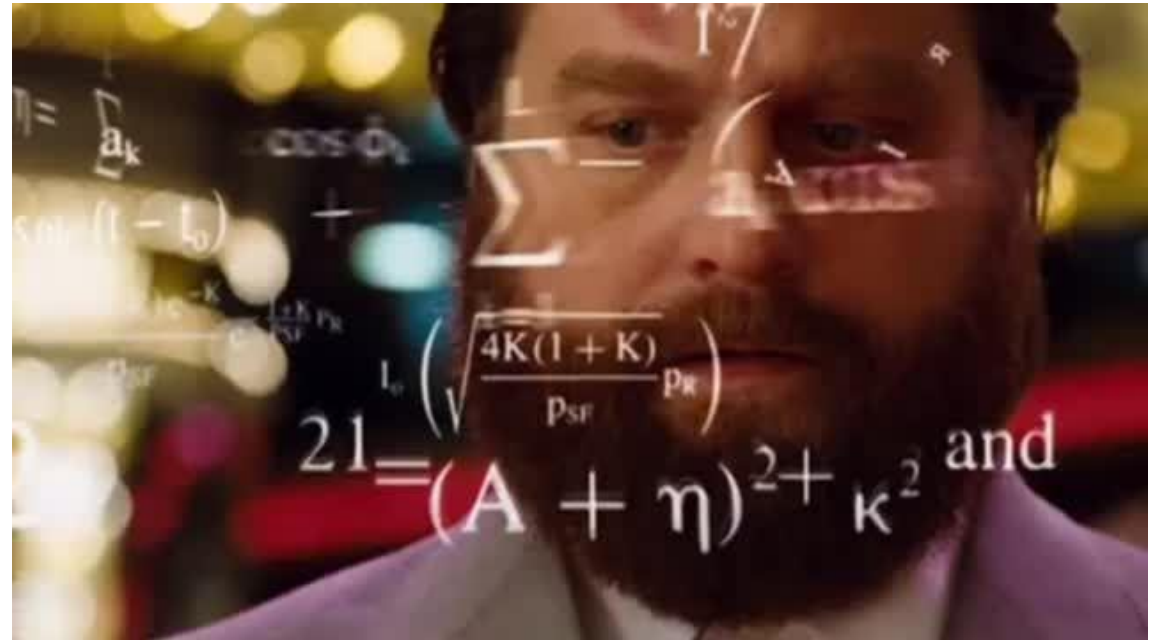
By tonikelo

MAKING-OF

The "shuffle algorithm" in 5 minutes

How does CoronaPoker shuffle?

| MODE | QUALITY |
|----------|---------|
| NORMAL | 9/10 |
| CASINO | 9.5/10 |
| PARANOID | 9.99/10 |



52! = 80658175170943878571660636856403766975289505440883277824000000000000

Fisher-Yates algorithm

5: We roll a 5-sided "die". (5 → we do nothing).

4: We roll a 4-sided "die". (1 → we swap the 4th for the 1st).

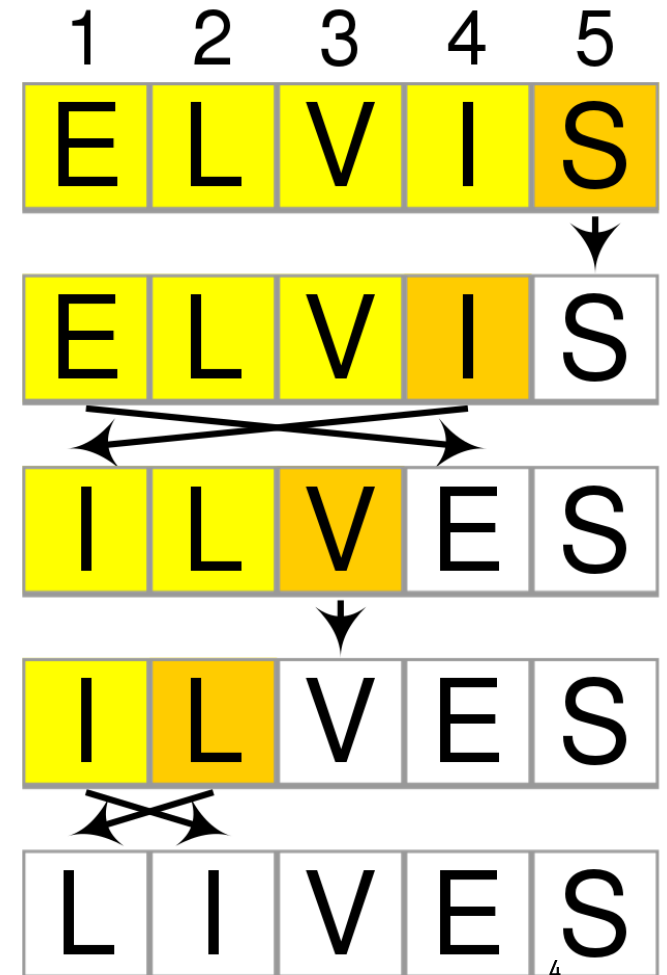
3: We roll a 3-sided "die". (3 → we do nothing).

2: We roll a 2-sided "die". (1 → we swap the 2nd for the 1st)

Note: although it may be "counter-intuitive", if the faces of the "die" were not reduced at each step of the algorithm, the permutations of the deck generated would not be equally likely, i.e., certain cards would tend to come out more often. The same would happen if we forced all the original elements to change places.

[\[More information\]](#)

END





CoronaPoker NORMAL MODE

- We start from an **ordered deck** of cards.
- The **Fisher-Yates** algorithm is used to shuffle it.
 - (This algorithm guarantees that all permutations of the deck that are generated are **random and equiprobable**).
- A cryptographically secure **pseudorandom** number generator (CSPRNG) **HASH DRBG SHA-512** is used to generate the random numbers required by Fisher-Yates.
 - (This generator has a secret internal state with more than enough size to guarantee that Fisher-Yates will be able to produce **any of the 52!** possible permutations).

CoronaPoker CASINO MODE

- On each hand, [RANDOM.ORG](#) is asked for a random permutation of 52 elements. [[GENERATE PERMUTATION RIGHT NOW](#)]
- RANDOM.ORG uses a true random number generator (TRNG) based on an atmospheric noise meter. The meter spits out a "stream" of 100% random ones and zeros that are scaled in a permutation [1,52]. [[More about random bit scaling](#)]
- It is capable of generating **any of the 52!** possible permutations of a poker deck in a **random and equiprobable** way.



CoronaPoker PARANOID MODE

- First we shuffle using the CASINO MODE and then we do the same using the NORMAL MODE, but this time starting from the permutation returned by RANDOM.ORG instead of a sorted deck.
- By combining two totally independent sources of entropy, any (very unlikely) deficiency of randomness is mutually neutralized.
- It gives us that extra peace of mind so we can focus on remembering that we haven't watched enough poker videos.



NO TE TE PIDO
QUE ME LO MEJORES,
¡IGUALAMELO!