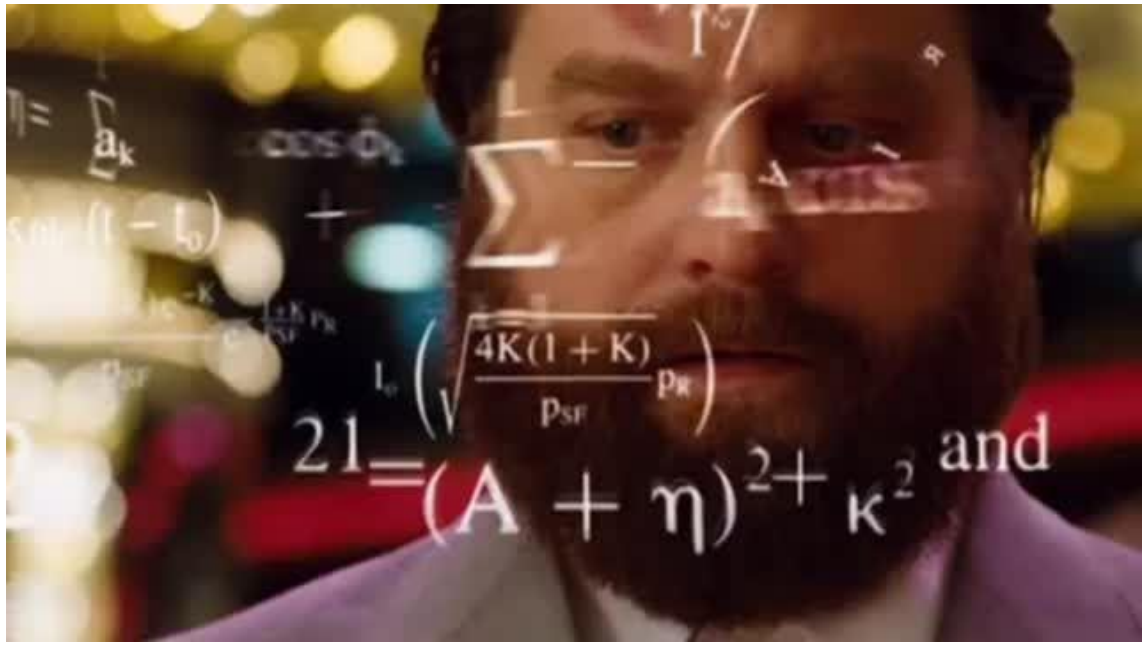
MAKING-OF

The "shuffle algorithm" in 5 minutes

How does CoronaPoker shuffle?

MODE	QUALITY
NORMAL	9.5/10
CASINO	9.9/10
PARANOID	9.999/10

How many different ways can a poker deck be ordered?



52 x 51 x 50 x 49 x 48 x … x 5 x 4 x 3 x 2 x 1 = 52!

52! = 80658175170943878571660636856403766975289505440883277824000000000000

Fisher-Yates algorithm

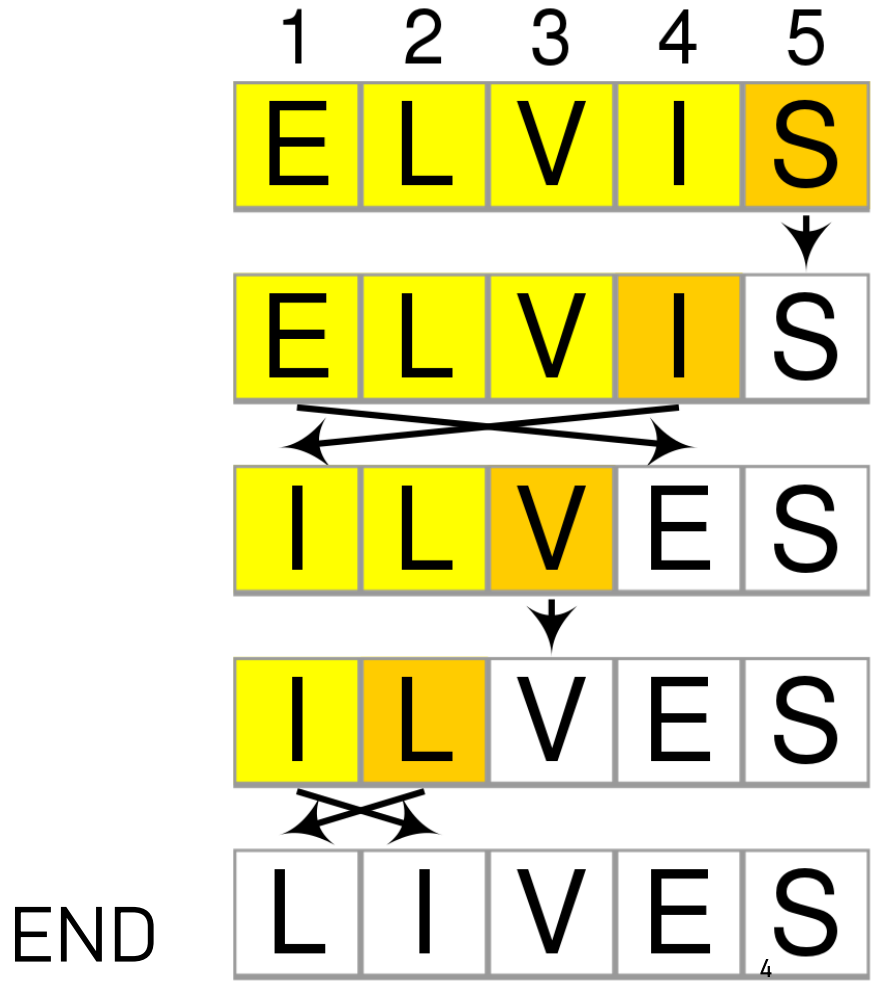
5: We roll a 5-sided "die". (5 -> we do nothing).

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]



CoronaPoker **NORMAL MODE**

- We start from an **ordered deck** of cards.
- The **Fisher-Yates** algorithm is used to shuffle it.
  - *O(n)* with "modern" Durstenfeld implementation.
- 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 in a **random and equiprobable** way).

CoronaPoker **CASINO MODE**

- On each hand, RANDOM.ORG is asked for a random permutation of 52 elements [1,52]. [GENERATE PERMUTATION RIGHT NOW]
- RANDOM.ORG uses a true random number generator (**TRNG**) based on **atmospheric noise**. A radio receiver connected to a computer, produces a **true random bit stream** which is subsequently scaled in order to generate a discrete random uniform distribution. [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 deck 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!