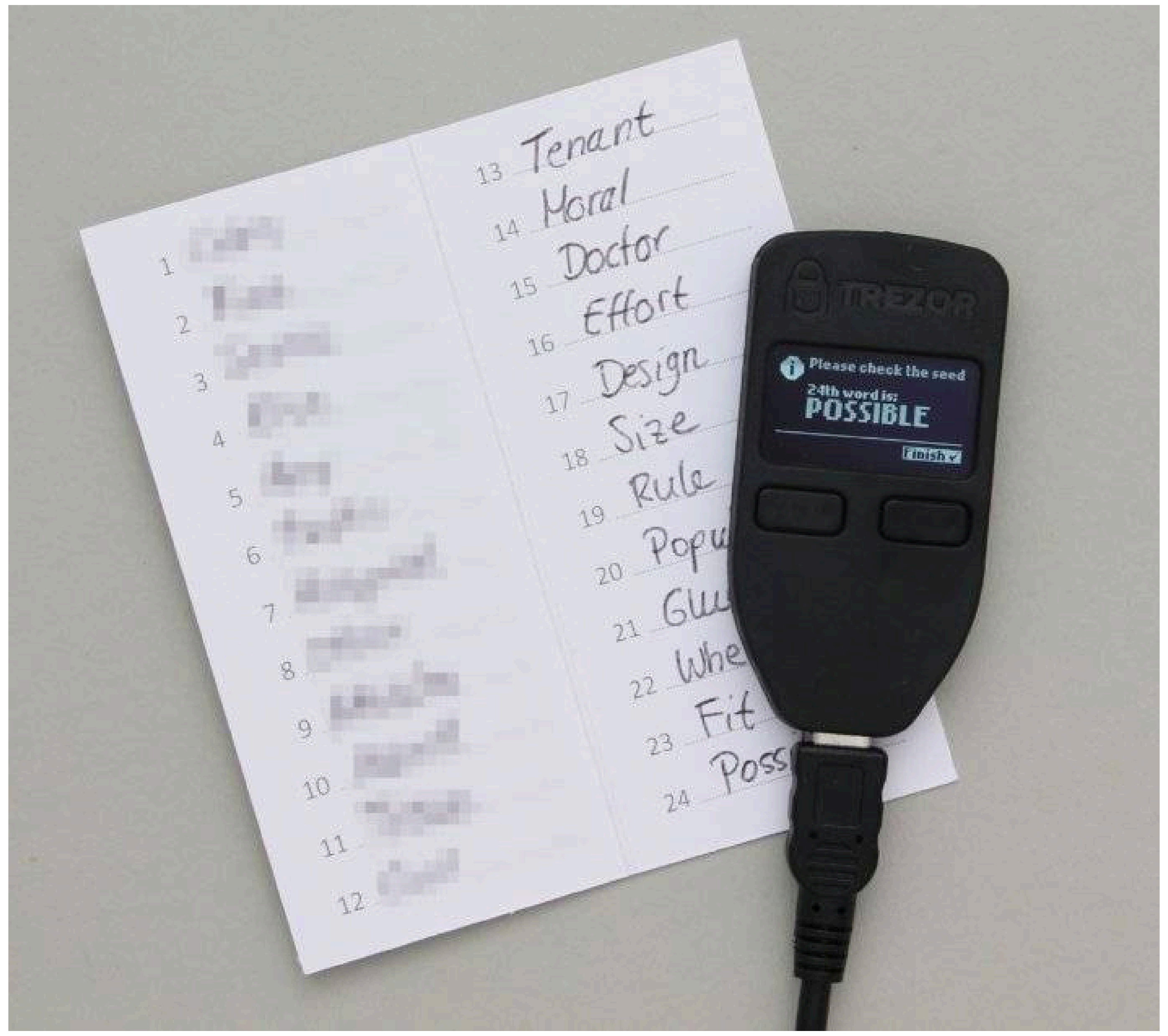
chaindeck

Your keys, your responsibility.

Chaindeck is used for storing bitcoin wallet seed phrases



Bitcoin gives the ability to self-custody. This means no banks or companies and is similar to holding cash at home.

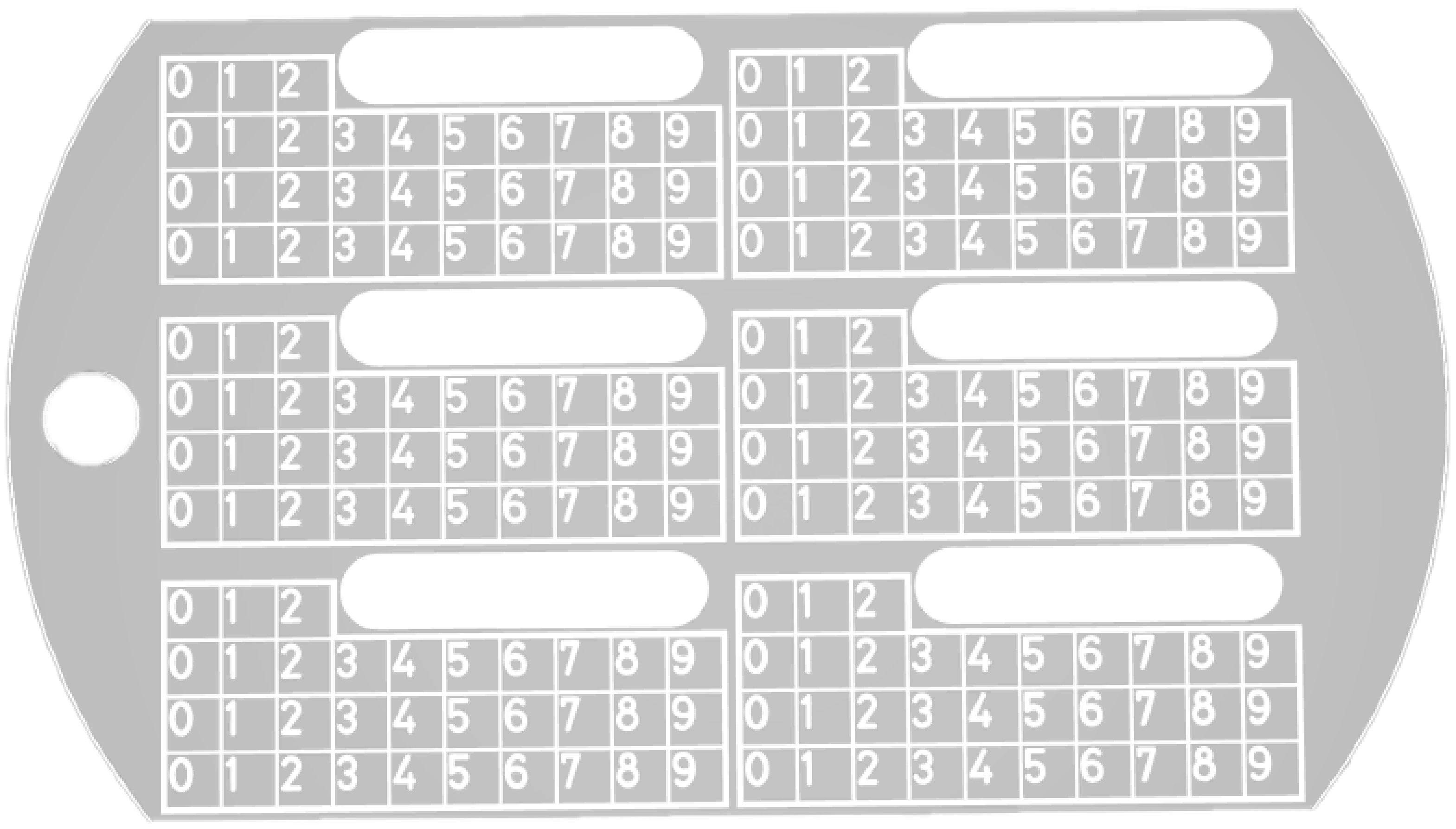
Non-custodial wallets are needed for self-custody. These wallets require a 12-24 word 'Secret Phrase' to backup the wallet.

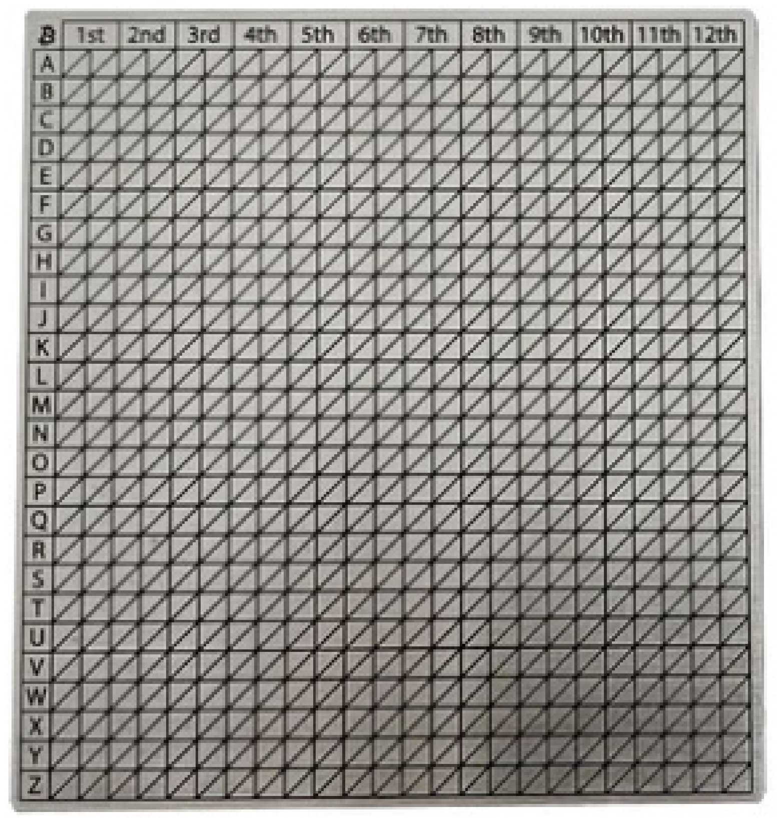
The Secret Phrase must be kept safe

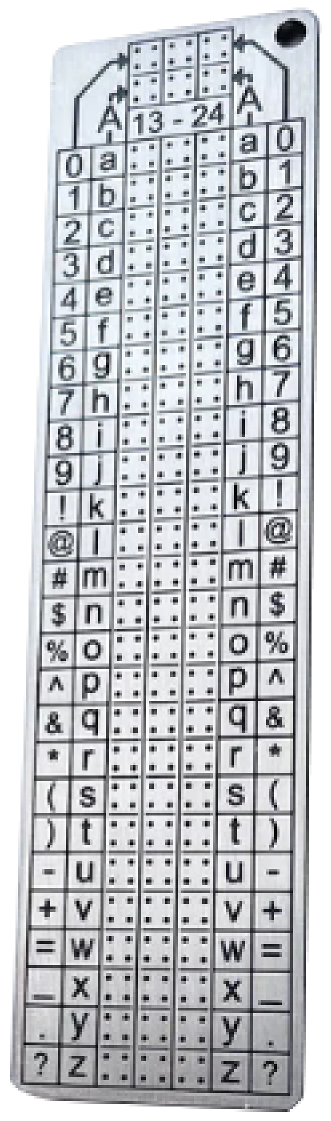
To ensure maximum security, the **Secret Phrase**:

- must not be lost over over a long time
- must never be in the view of cameras
- must never be accessible to strangers
- must never be digitized e.g. saved on a laptop, DropBox, password manager, Google Drive etc.

Current best way is etching the Secret Phrase on metal







Click here for the results of stress testing 22 new metal devices for storing seed phrase backups.

WHAT IS CHAINDECK? Chaindeck is a deck of 100 cards used to store a Secret Phrase. Shuffling the cards scrambles the Secret Phrase. The specific way the cards are Sorted, Flipped and Rotated is called a CHAIN.

HOW TO CHAINDECK? Chain the deck using your 3-digit PIN. Write your Secret Phrase to the side of the deck using a pen. Shuffle before safely storing your deck.

HOW TO RETRIEVE RECOVERY PHRASE? Chaining your deck using the same method will reveal secret phrase written on the side of your deck.

STEP 1 Group Cards

STEP 2 Sort Each Group

STEP 3 Combine Groups

STEP 4 Rotate Cards

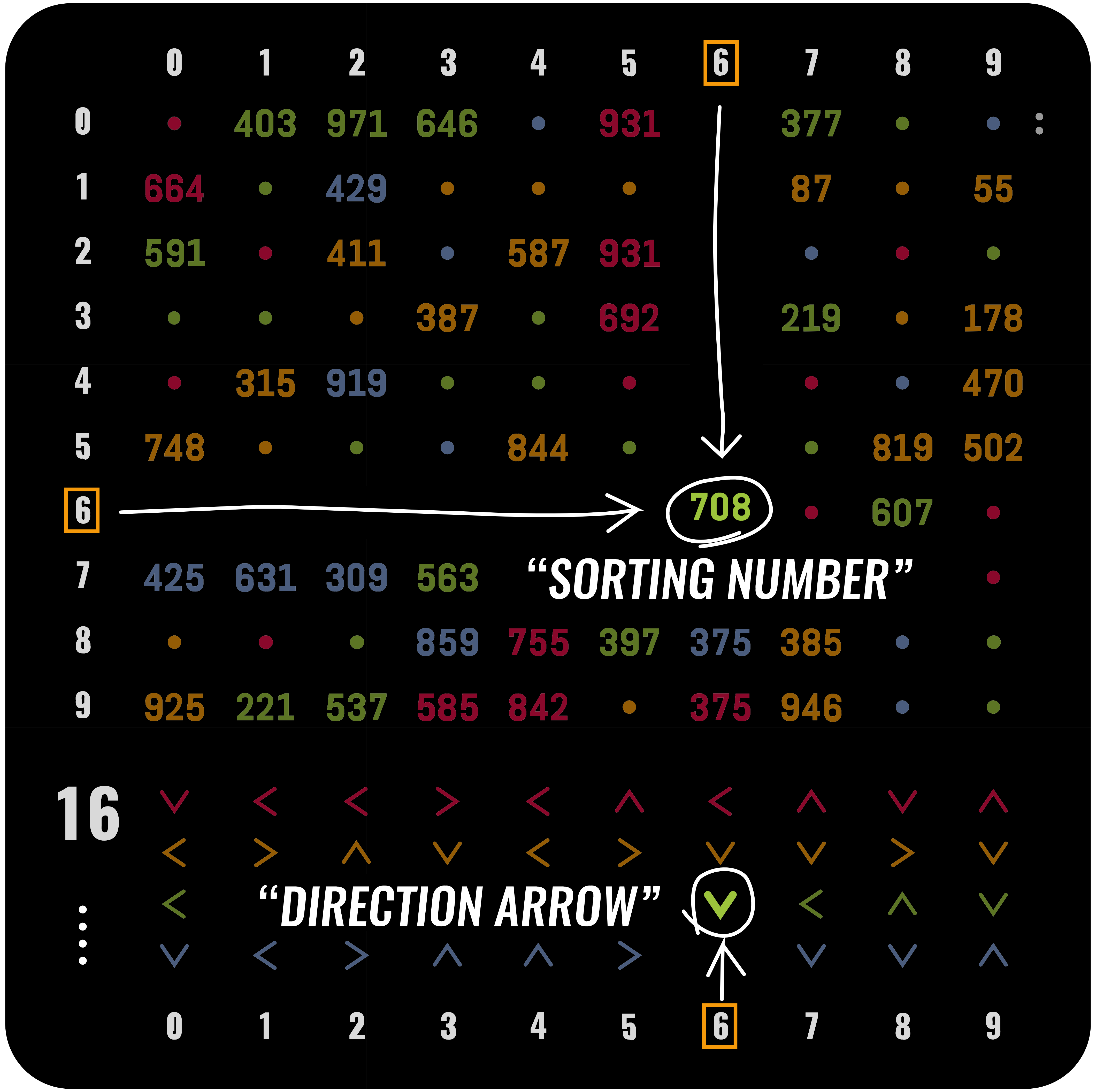
STEP 5 Write Secret Phrase

STEP 6 Shuffle Cards And Store Safely

SORTING NUMBER Each card has a unique Sorting Number which you can find only on one side of the card. Use the first digit of your PIN to find the correct row, and the second digit of your PIN for the correct column. If the sorting number is missing, flip the card to find it on th other side.

DIRECTION ARROW Use the third digit of your PIN and the color of the Sorting Number to pick the correct Direction Arrow. If your Sorting Number is red, your direction arrow is also red. See example on next slide for PIN: 666

Example PIN 666



SECOND DIGIT

FIRST DIGIT

THIRD DIGIT

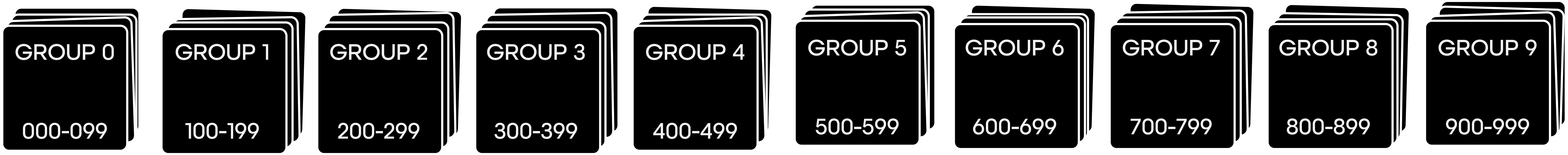
"SORTING NUMBER"

"DIRECTION ARROW"

	0	1	2	3	4	5	6	7	8	9
0	●	403	971	646	●	931		377	●	●
1	664	●	429	●	●	●		87	●	55
2	591	●	411	●	587	931		●	●	●
3	●	●	●	387	●	692		219	●	178
4	●	315	919	●	●	●		●	●	470
5	748	●	●	●	844	●		●	819	502
6							708	●	607	●
7	425	631	309	563						●
8	●	●	●	859	755	397	375	385	●	●
9	925	221	537	585	842	●	375	946	●	●

16	∨	<	<	>	<	∧	<	∧	∨	∧
	<	>	∧	∨	<	>	∨	∨	>	∨
⋮	<						∨	<	∧	∨
	∨	<	>	∧	∧	>		∨	∨	∧
	0	1	2	3	4	5	6	7	8	9

STEP 1 Group Cards



GROUP 0 000-099

GROUP 1 100-199

GROUP 2 200-299

GROUP 3 300-399

GROUP 4 400-499

GROUP 5 500-599

GROUP 6 600-699

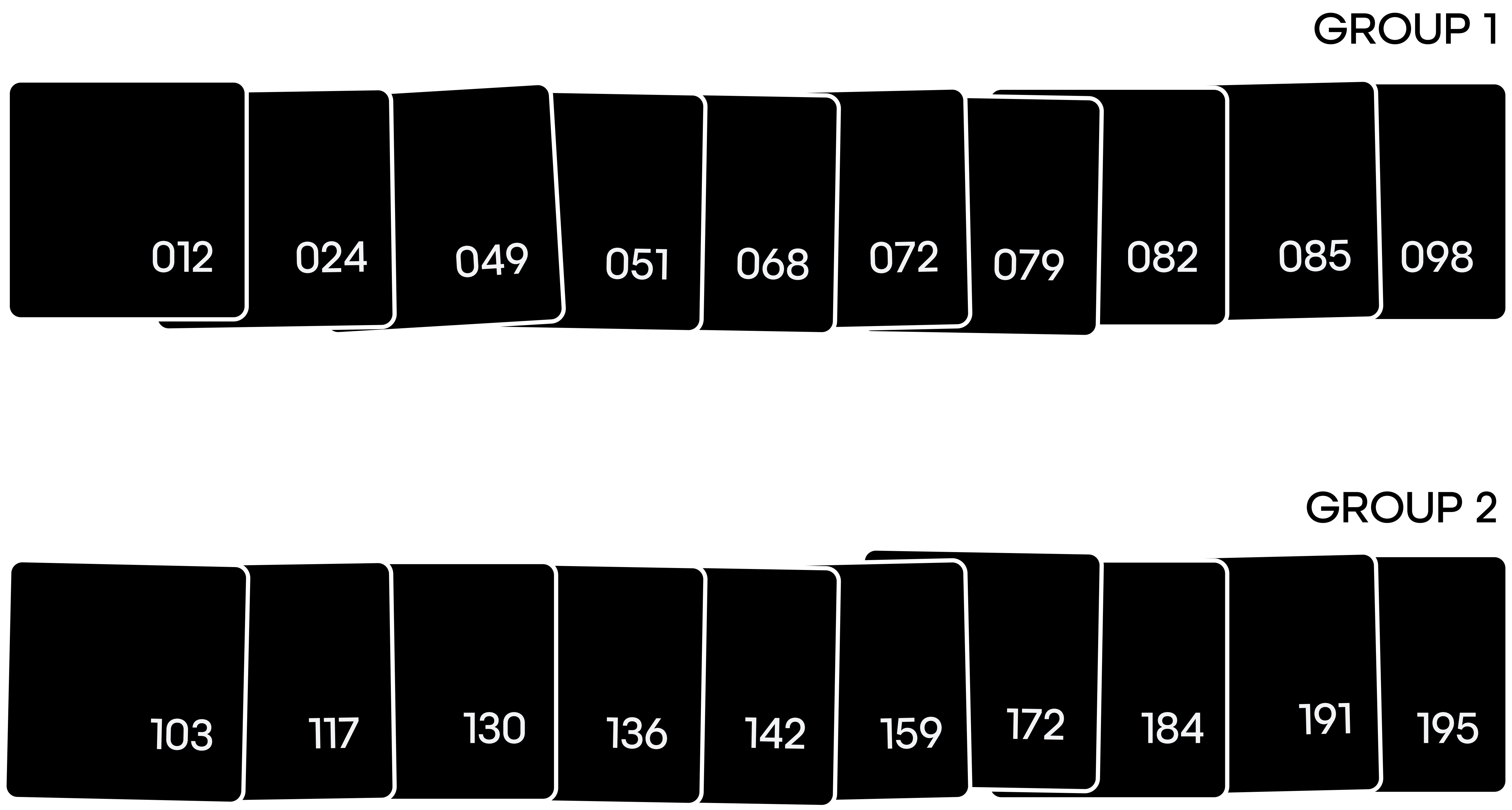
GROUP 7 700-799

GROUP 8 800-899

GROUP 9 900-999

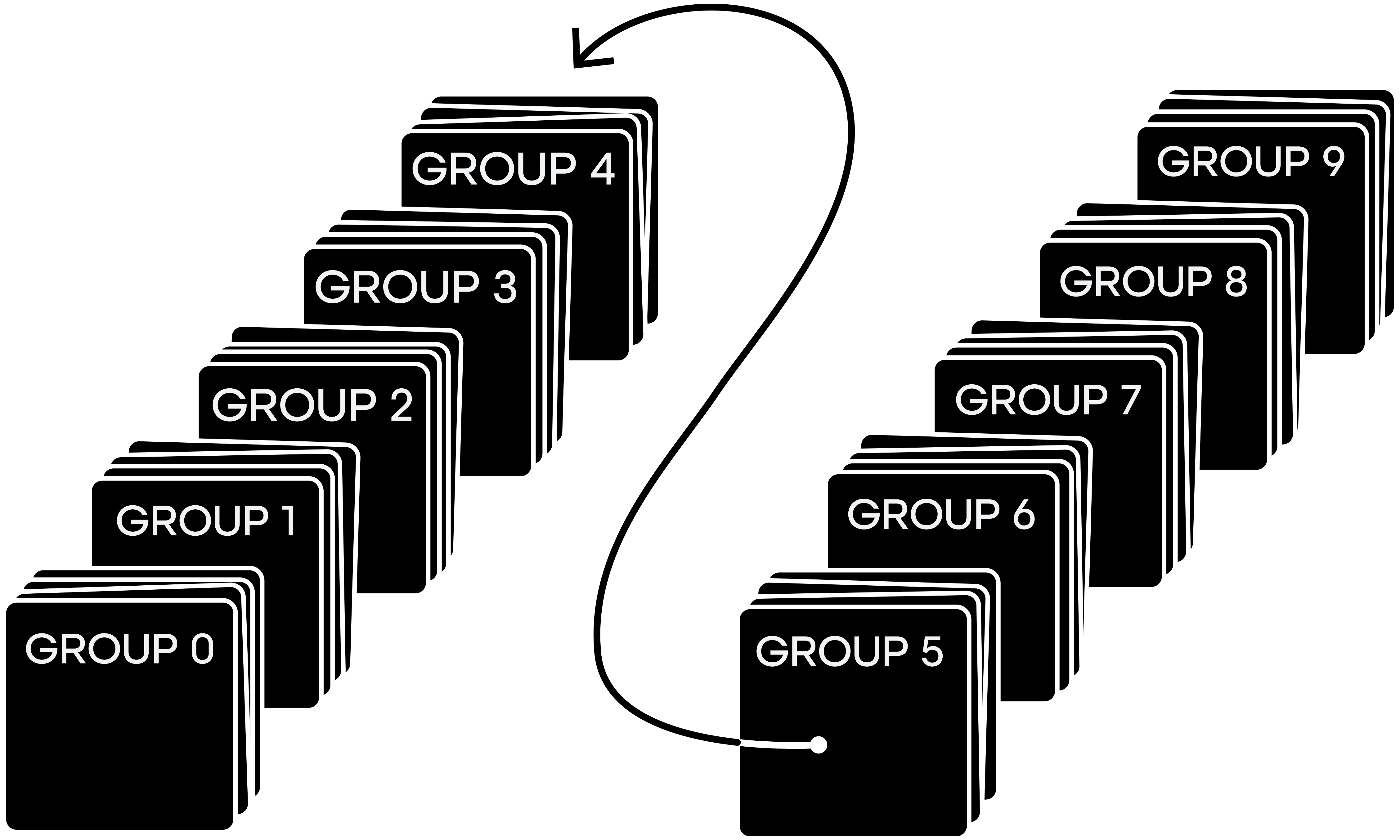
Find the Sorting Number on each card and place the cards in groups based on the first digit of their Sorting Number. You will end up with 10 groups.

STEP 2 Sort Each Group



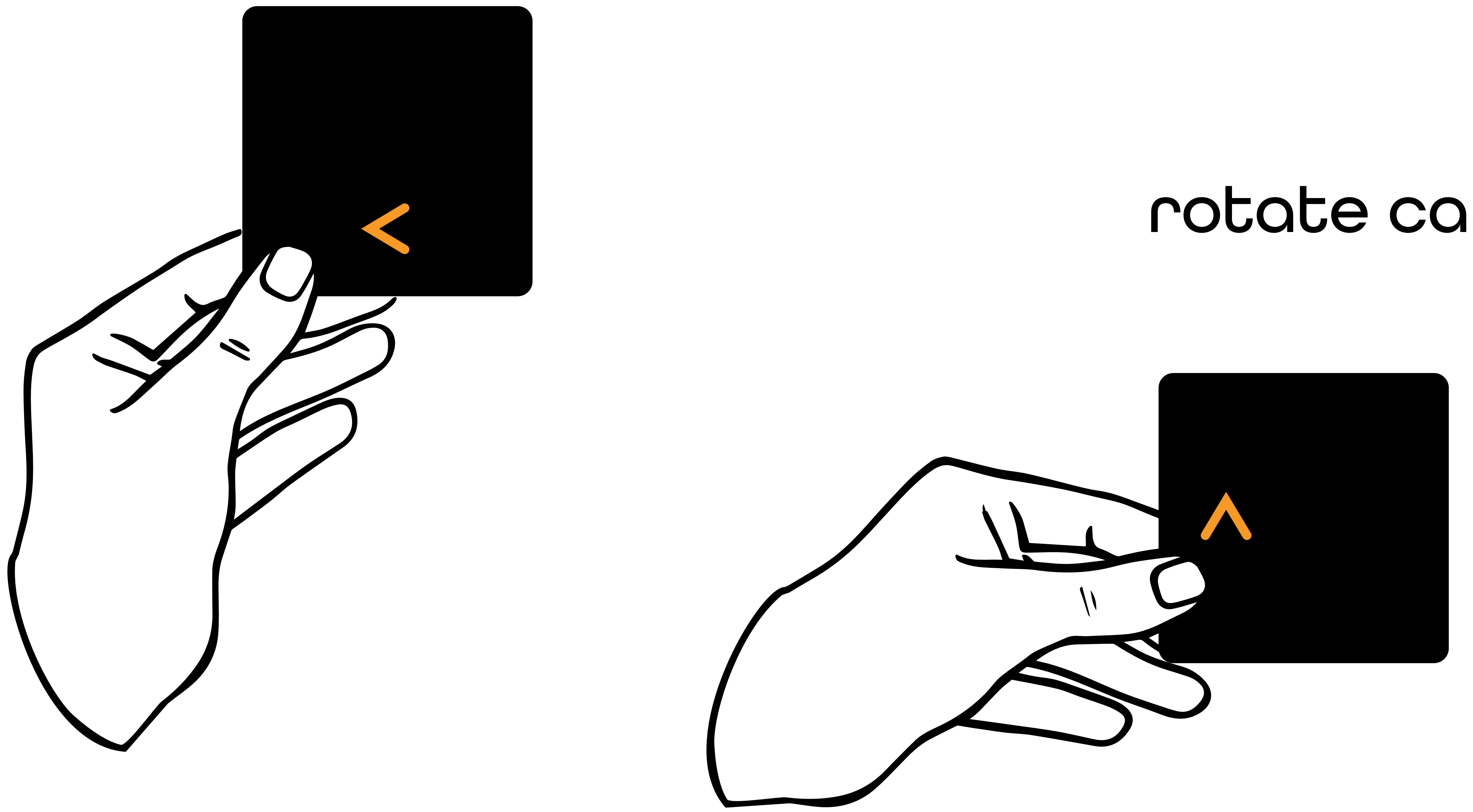
Sort the cards in each group so that the card with the smallest Sorting Number is the first, and the card with the highest Sorting Number is the last within each group. (Your Sorting Numbers will be different from what is shown here.)

STEP 3 Combine Groups



Combine the groups from small to high. Group 0 (000-099) should be first and Group 9 (900-999) should be last in the deck.

STEP 4 Rotate Cards

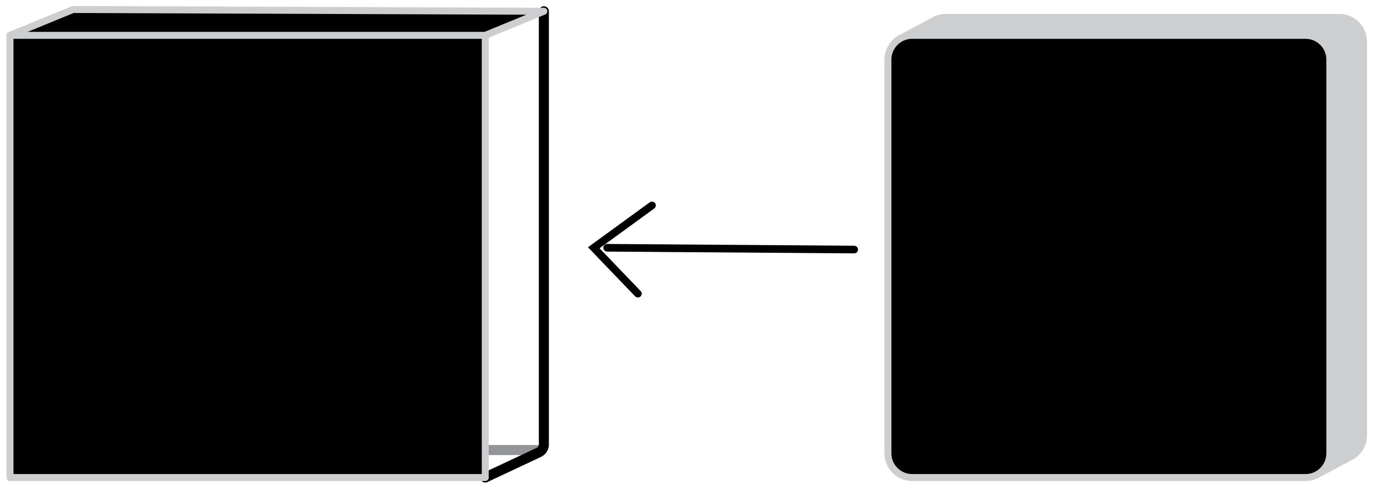


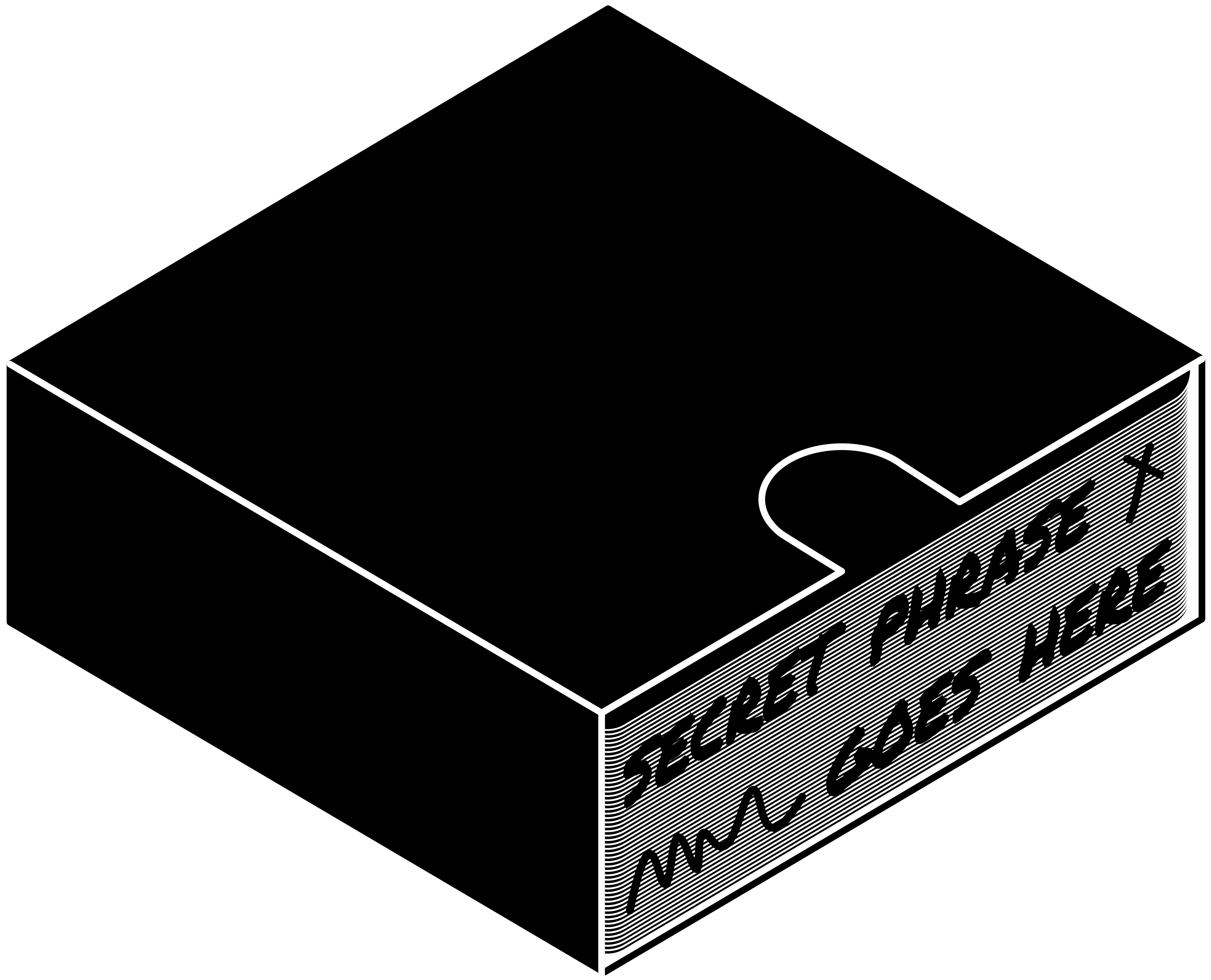
If arrow points left;

rotate card 90° clock-wise

Rotate each card so that the Direction Arrow points up. Do not change the order or flip the cards. If the arrow is already pointing up, you don't need to rotate.

STEP 5 Write Secet Phrase

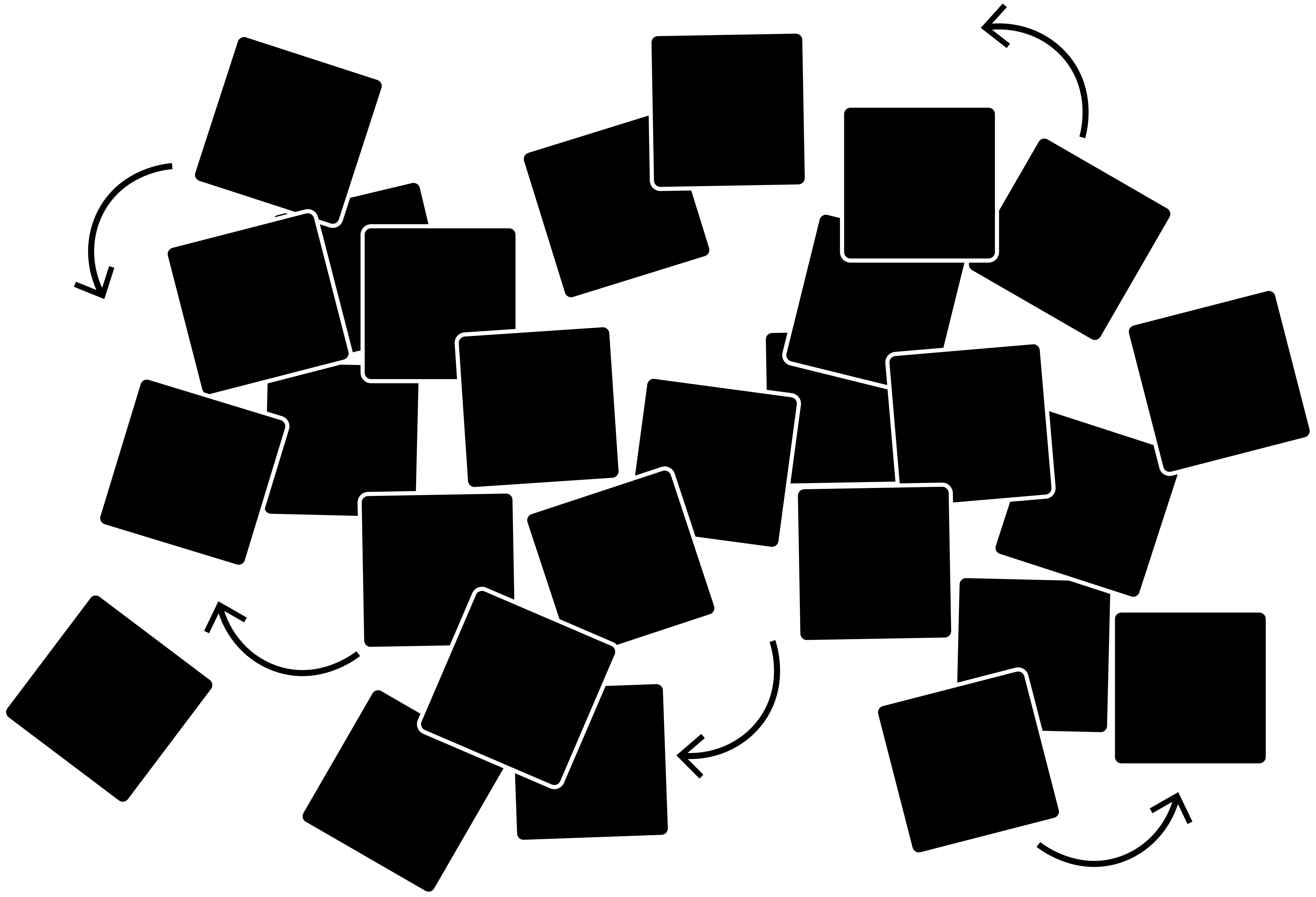


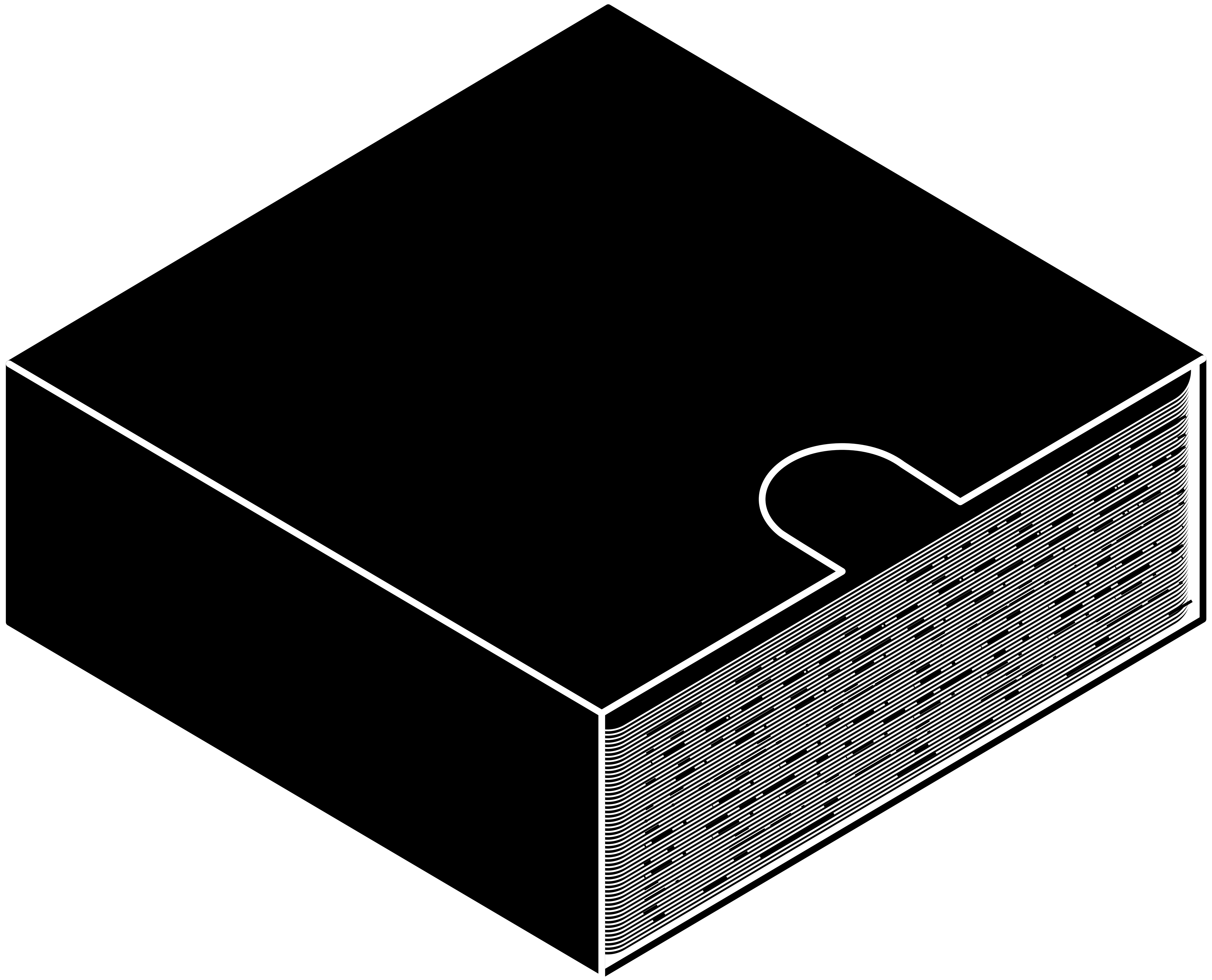


Placing the deck in the sleeve will help hold the deck in place while exposing a single side to write on. Using a medium tip marker, use one side of the deck to write your Secret Phrase.

If you run out of space and have to switch to another side of the deck, make sure to mark the new side as such.

STEP 6 Shuffle Cards





FLIP ROTATE MIX It is important to shuffle the cards in a way that maximizes the randomness of the outcome. Once shuffled you can store your deck safely.

Chaindeck Advantages

ASTRONOMICAL ARRANGEMENTS

Chaindeck has $2x10^{247}$ card arrangements.

NON-DIGITAL

Internet, phone, computer, batteries, etc. not required at any step.

DELATED ACCESS

If stolen, it takes time and effort to access the Secret Phrase.

MODULAR

Decks can be combined and split for more security.

HANDWRITTEN

Any character, symbol, language is possible.

Chaindeck Is Not Perfect

TAKES TIME

It takes 15 minutes to set up and 10 minutes to retrieve the Secret Phrase. Alternatives that are faster to set up are less secure.

PIN MUST BE REMEMBERED

Chaindeck is designed so that Secret Phrase can only be accessed by those who know the PIN.

NOT FIRE OR WATER PROOF

Chaindeck can be stored in a safe or protective box.

SECRET PHRASE MAY BE EVENTUALLY RETRIEVED

The owner can use custom arrangements, false markings, or multiple decks to increase security of the Secret Phrase.

Chaindeck Use-cases

STORING SEED PHRASE

Hardware wallets (Ledger, Trezor, Coldcard, etc.)

Software wallets (Mycelium, Exodus, Coinomi, etc.)

PASSWORD STORAGE

Password manager backups

Master passwords

API keys

SECRET MESSAGES

Romantic messages

Time capsules

Delayed messages (by sending PIN later)

What’s Included

100-CARD CHAINDECK

The cards that are arranged to store the Secret Phrase.

INFORMATION BOOKLET

Folding booklet that explains how to use Chaindeck.

SLIDING TUCK BOX AND CARDBOARD BOX

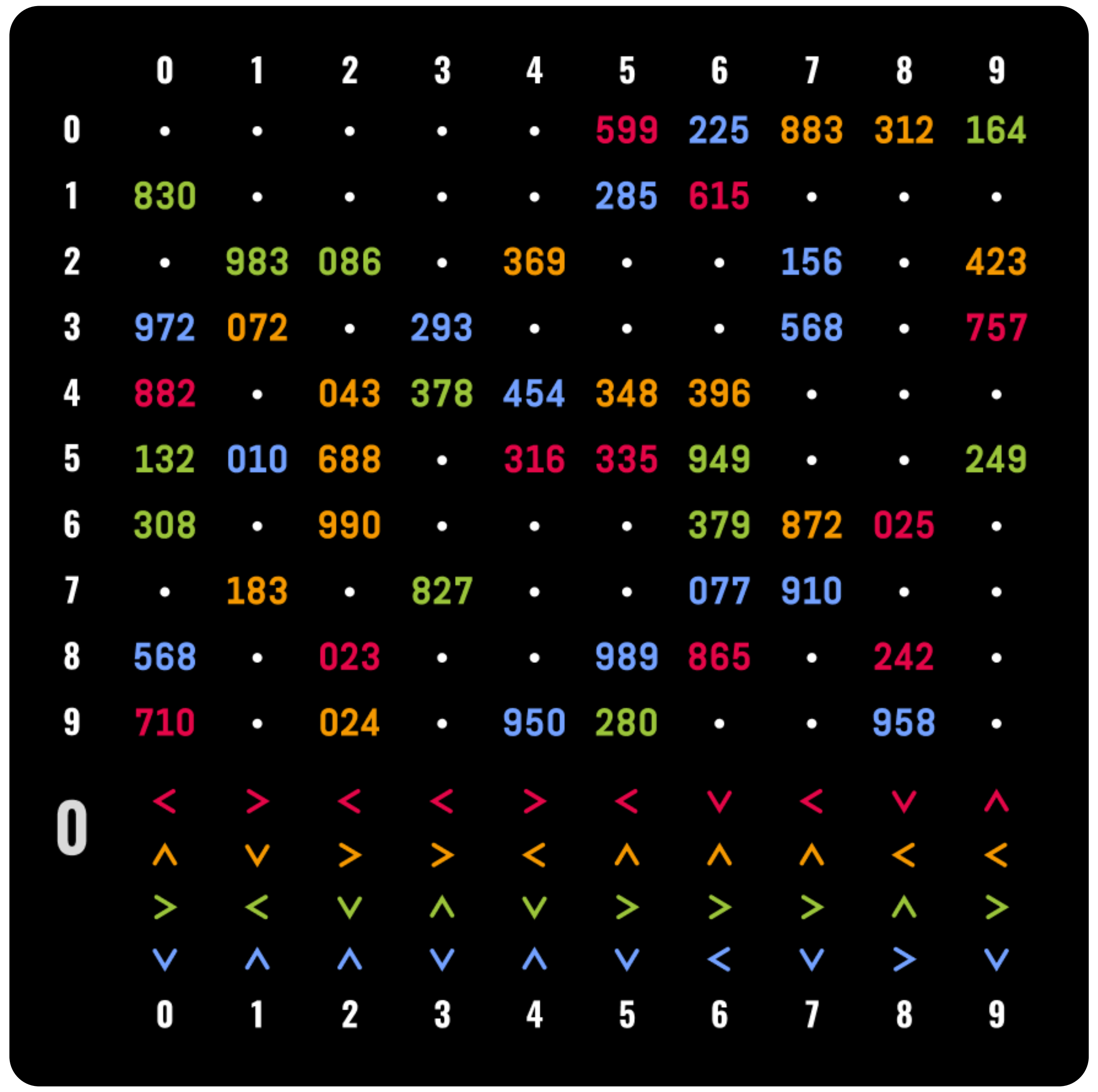
Tuck box helps hold the cards to write the Secret Phrase, and goes in the Cardboard Box.

TAMPER SEAL AND NOVELTY CARDS

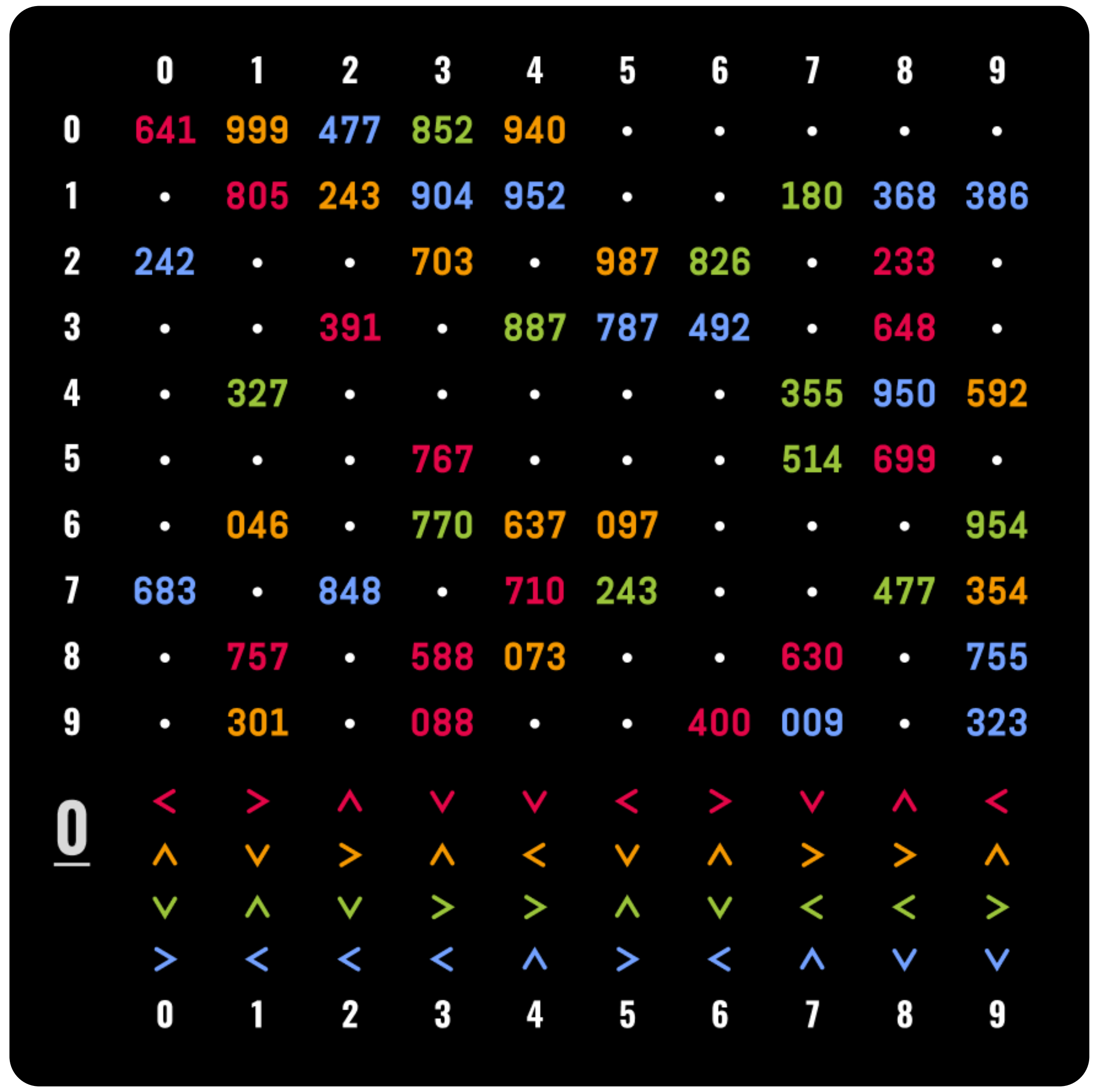
Tamper-evident seals and a few novelty cards.

Q&A

Card #0

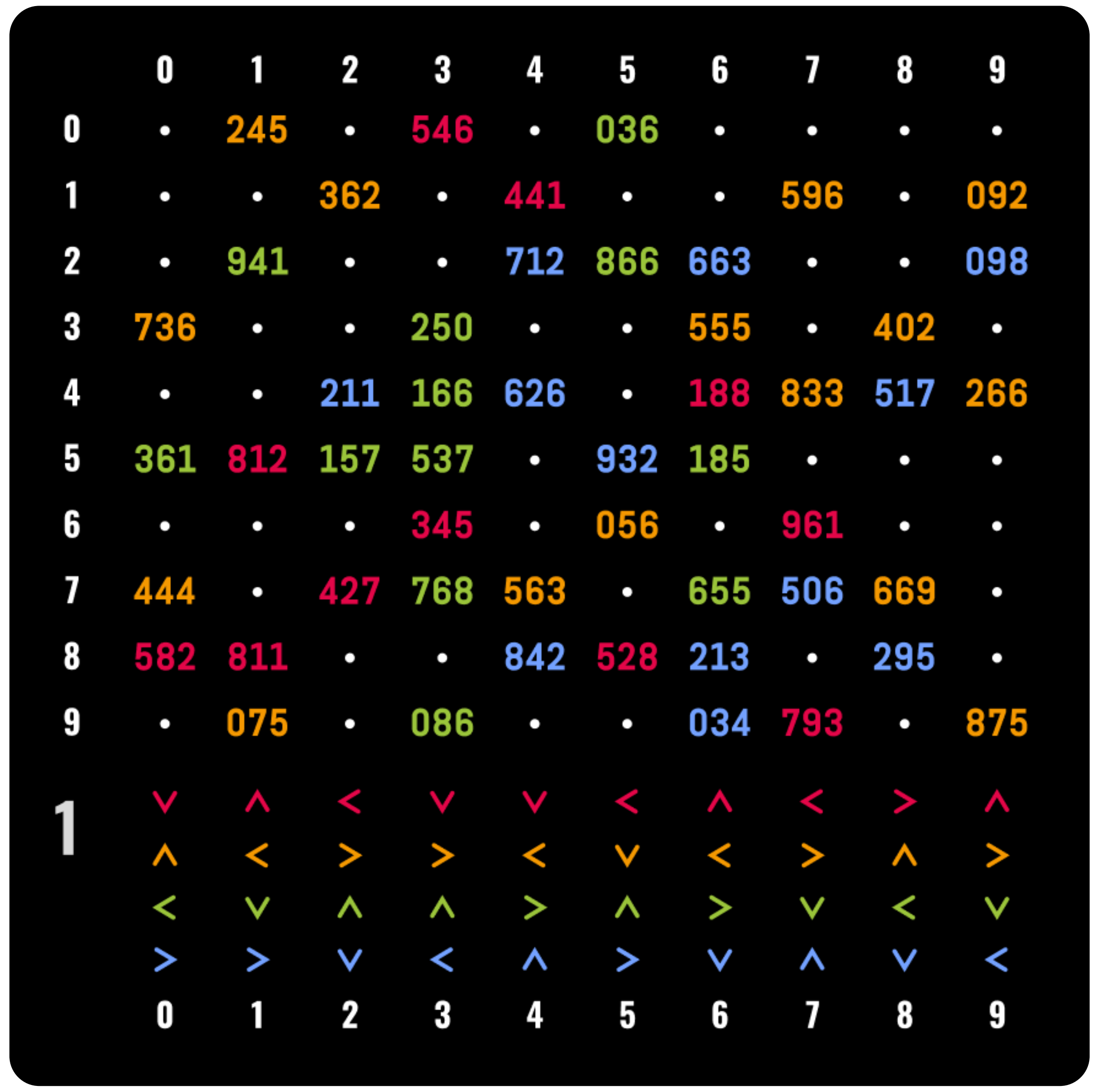


	0	1	2	3	4	5	6	7	8	9
0	•	•	•	•	•	599	225	883	312	164
1	830	•	•	•	•	285	615	•	•	•
2	•	983	086	•	369	•	•	156	•	423
3	972	072	•	293	•	•	•	568	•	757
4	882	•	043	378	454	348	396	•	•	•
5	132	010	688	•	316	335	949	•	•	249
6	308	•	990	•	•	•	379	872	025	•
7	•	183	•	827	•	•	077	910	•	•
8	568	•	023	•	•	989	865	•	242	•
9	710	•	024	•	950	280	•	•	958	•
0	<	>	<	<	>	<	∨	<	∨	∧
	∧	∨	>	>	<	∧	∧	∧	<	<
	>	<	∨	∧	∨	>	>	>	∧	>
	∨	∧	∧	∨	∧	∨	<	∨	>	∨
	0	1	2	3	4	5	6	7	8	9

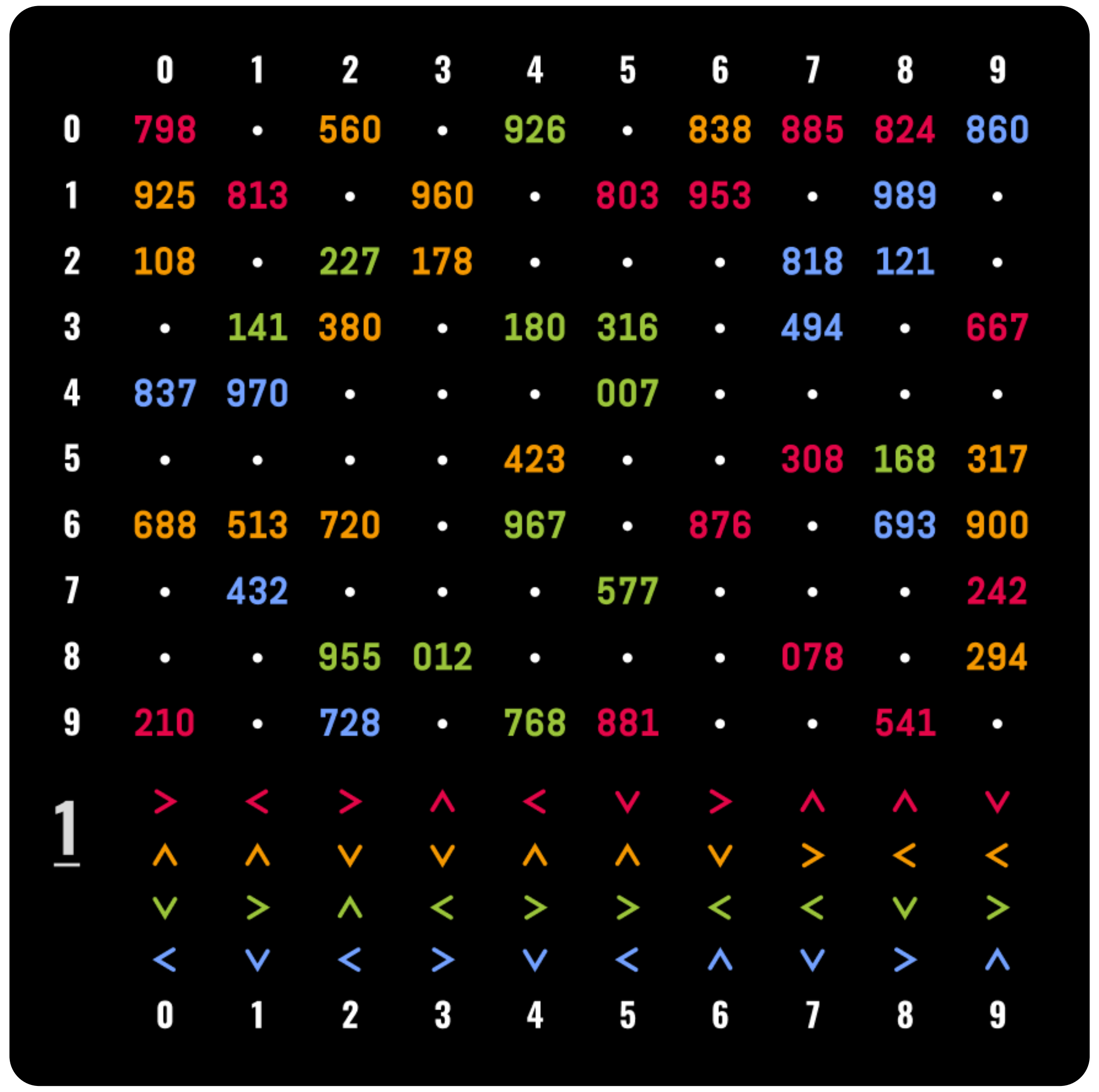


	0	1	2	3	4	5	6	7	8	9
0	641	999	477	852	940	•	•	•	•	•
1	•	805	243	904	952	•	•	180	368	386
2	242	•	•	703	•	987	826	•	233	•
3	•	•	391	•	887	787	492	•	648	•
4	•	327	•	•	•	•	•	355	950	592
5	•	•	•	767	•	•	•	514	699	•
6	•	046	•	770	637	097	•	•	•	954
7	683	•	848	•	710	243	•	•	477	354
8	•	757	•	588	073	•	•	630	•	755
9	•	301	•	088	•	•	400	009	•	323
0	<	>	∧	∨	∨	<	>	∨	∧	<
	∧	∨	>	∧	<	∨	∧	>	>	∧
	∨	∧	∨	>	>	∧	∨	<	<	>
	>	<	<	<	∧	>	<	∧	∨	∨
	0	1	2	3	4	5	6	7	8	9

Card #1



	0	1	2	3	4	5	6	7	8	9
0	•	245	•	546	•	036	•	•	•	•
1	•	•	362	•	441	•	•	596	•	092
2	•	941	•	•	712	866	663	•	•	098
3	736	•	•	250	•	•	555	•	402	•
4	•	•	211	166	626	•	188	833	517	266
5	361	812	157	537	•	932	185	•	•	•
6	•	•	•	345	•	056	•	961	•	•
7	444	•	427	768	563	•	655	506	669	•
8	582	811	•	•	842	528	213	•	295	•
9	•	075	•	086	•	•	034	793	•	875
1	∨	∧	<	∨	∨	<	∧	<	>	∧
	∧	<	>	>	<	∨	<	>	∧	>
	<	∨	∧	∧	>	∧	>	∨	<	∨
	>	>	∨	<	∧	>	∨	∧	∨	<
	0	1	2	3	4	5	6	7	8	9



	0	1	2	3	4	5	6	7	8	9
0	798	•	560	•	926	•	838	885	824	860
1	925	813	•	960	•	803	953	•	989	•
2	108	•	227	178	•	•	•	818	121	•
3	•	141	380	•	180	316	•	494	•	667
4	837	970	•	•	•	007	•	•	•	•
5	•	•	•	•	423	•	•	308	168	317
6	688	513	720	•	967	•	876	•	693	900
7	•	432	•	•	•	577	•	•	•	242
8	•	•	955	012	•	•	•	078	•	294
9	210	•	728	•	768	881	•	•	541	•
1	>	<	>	∧	<	∨	>	∧	∧	∨
	∧	∧	∨	∨	∧	∧	∨	>	<	<
	∨	>	∧	<	>	>	<	<	∨	>
	<	∨	<	>	∨	<	∧	∨	>	∧
	0	1	2	3	4	5	6	7	8	9

Front

Back

chaindeck

Your keys, your responsibility.

Appendix 1. Alternative Methods to Use Chaindeck

METHOD	DESCRIPTION	SETUP	RECOVERY	SECURITY	COMPLEXITY
FACTORY CHAIN	Use the cards with the arrangement they come in. Deck is stored shuffled.	2 min	7 min	Low	Easy
PIN	Use a 3-digit PIN to arrange the cards. This is the default method.	15 min	10 min	Medium	Medium
SHUFFLE-RECORD	Randomly shuffle the deck, record the arrangement of the cards. Must have the record to recover.	15+ min	15 min	Medium	Medium
OWNDER-DEFINED	Use a unique way to arrange the cards, such as using the random numbers and markings on the cards.	20+ min	15+ min	High	Difficult

Appendix 2. Chaindeck Math

Using the 3-digit PIN, there are 1,000 unique arrangements available. Owner's PIN will correspond to one of these.

With a 100-card Chaindeck, there are 2^{100} x 4^{100} x 100! / 8 possible arrangements, which equals 2.4×10^{247}

There are 8×10^{67} possible ways to shuffle a 52-card deck of cards.

There are 10^{120} possible games of chess.

There are 10^{170} possible games of Go.

It takes 50-71 minutes to try 10 consecutive PINs. On average, it would take about 500 tries and 41-59 hours to guess the correct PIN.

It would take up to five days of non-stop card arranging to find the correct PIN.

Appendix 3. Secret Phrase Writing Best Practices

Each word should use about 5-10 cards.

The words can be used to find the following cards, so using too many should be avoided.

The order of the words should be obvious.

False markings should be made after a good shuffle, and process repeated a few times.

The deck can be arranged for another PIN and a fake Secret Phrase could be written in empty spaces on the sides of the deck.

The color-based lookup method makes figuring-out the PIN from a few correctly arranged cards very difficult.

chaindeck

Your keys, your responsibility.