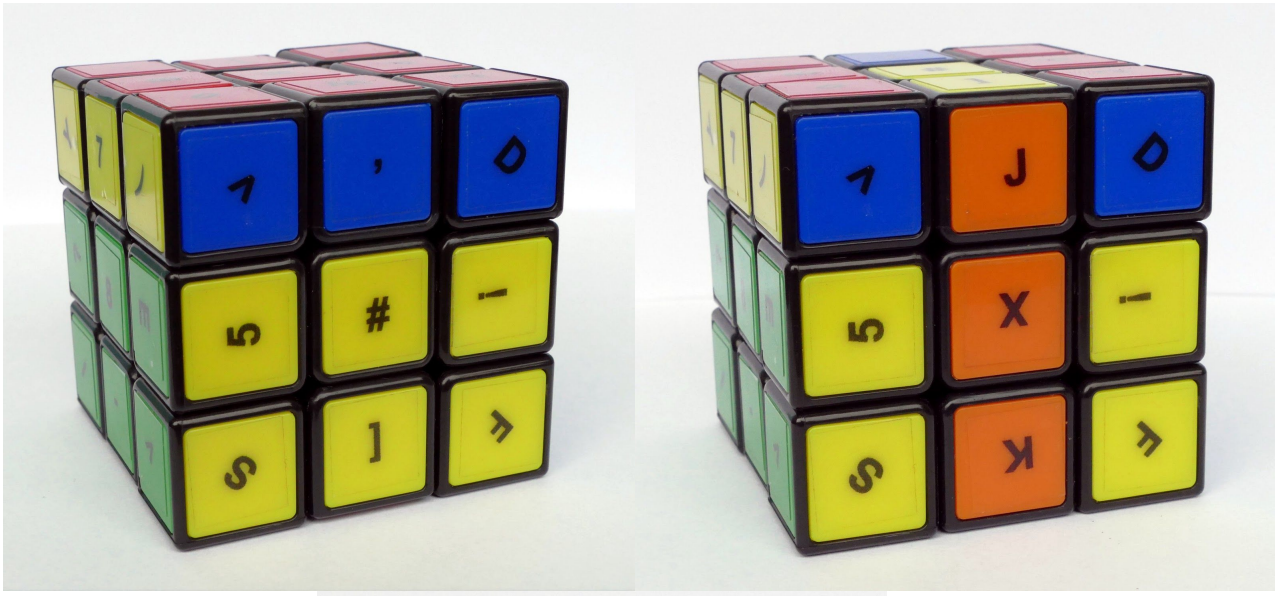
## Creating a password

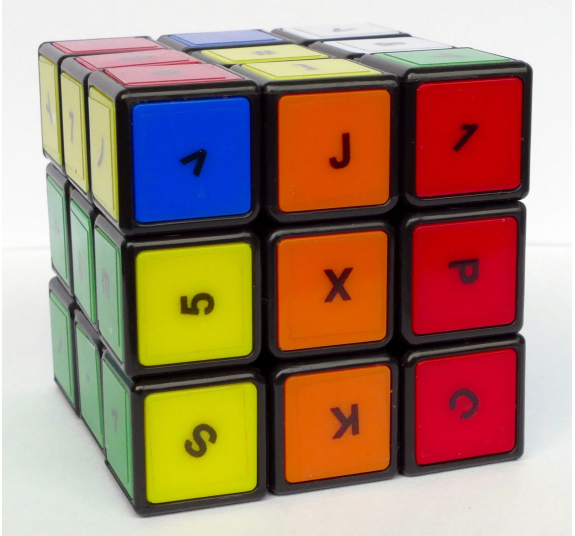
**1.**

Identify the front and top of the cube for specific account (such as e-mail access). For example, we select yellow (front) — red (top). Note that the characters are always located from the center to the outer edge of the cube. During the testing, we found out that such situated characters are easier to read and thus avoids confusion of axially symmetrical characters such as parentheses.

**2.**

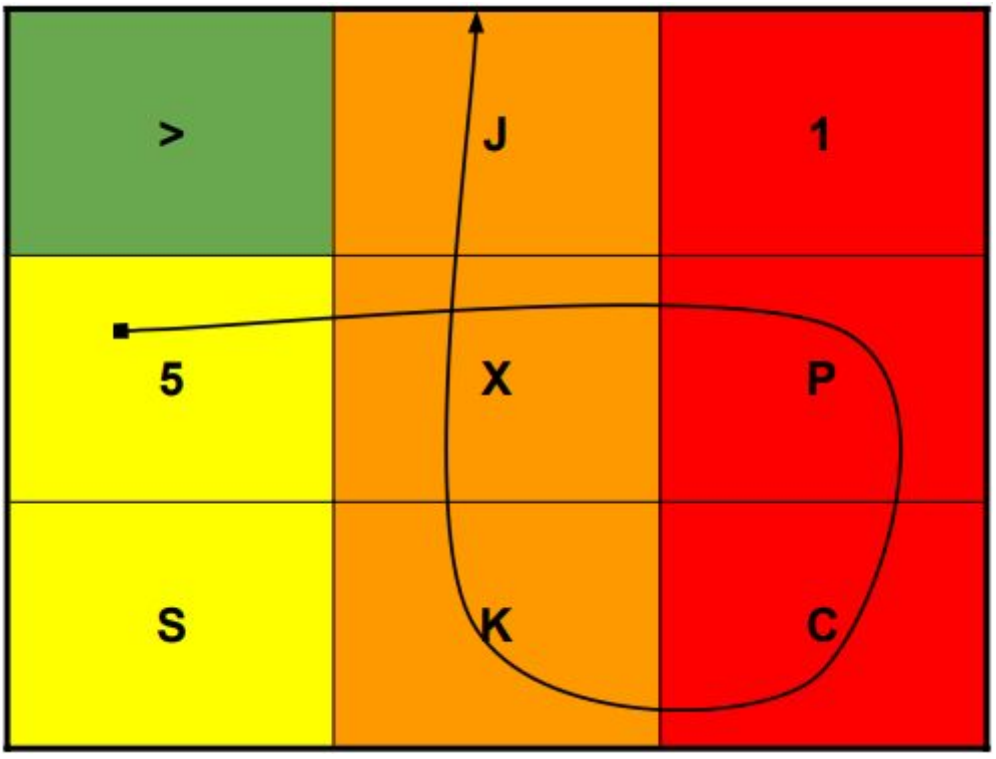
Make your own algorithm to “shuffle” the dice. 3–5 different turns are sufficient; your motor memory will take care of the movement over time, so you don’t have to worry about forgetting your algorithm. We choose, for example, the rotation **U r R ‘** — ie we turn the upper row once to the left, the middle column turn once up, the right column turn once down. This algorithm will be used for all passwords.





**3.**

Make your own “gesture” to read each character. This is the same principle as a gesture to unlock the phone screen. Using the gesture, we create a basic hash: “**5xpckxj**”. This gesture will be used to create all passwords.



**4.**

Make your own password of 5–7 characters and a system to put it into a hash from the cube. It is necessary that the password contains at least one uppercase letter, because we read all the letters from the cube as lowercase and therefore we would miss the security element.

For example, we choose a password with five characters: "**hC25@**". The hash insertion system will be as follows (the dot represents the letter/number/ special character from hash):

Insertion system: "**..hC....25.@**"

Depending on your system, you will enter this password equally into all hashes. It is not recommended to insert it whole at once, always divide it into at least two parts.

The resulting password for your email is "**5xhCpckx25j@**"

For the next account, you choose a different front and top of the cube and do the same. You will use the same system of rotating the cube, same gesture, and password insertion.