

# Sichere Passwörter/Muster

## Häufig genutzte Passwörter

Passwörter können heutzutage durch immer mehr Rechenleistung immer einfacher geknackt werden. Dabei sind kurze und vorhersehbare Passwörter natürlich deutlich leichter zu erraten als längere und komplexere.

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &amp;3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p><math>2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

In den meisten Fällen muss man davon ausgehen, dass eine Angreiferin **unendlich viele Versuche** hätte, um ein Passwort zu erraten. Sie könnte einen **sehr leistungsfähigen Computer** benutzen und diesen mit Wörterbüchern und Zeichen aus allen möglichen Sprachen füttern, und den Computer alle möglichen Kombinationen ausprobieren lassen. Dieses Vorgehen nennt man

auch *Brute Force*, übersetzt *rohe Gewalt*. Ein solcher Computer könnte auch **gezielt Kombinationen von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen ausprobieren**.

Vor solchen Methoden sind von Menschen ausgedachte Passwörter in der Regel nicht sicher. Um sich Passwörter merken zu können, helfen vertraute Muster, Laute, Zeichenfolgen oder Wörter. Hinzu kommt, dass sich die meisten Menschen nur eine begrenzte Anzahl zufälliger Zeichenketten merken können.

Das führt dazu, dass Menschen oft den Fehler machen dieselben Passwörter für verschiedene Webseiten benutzen. Nicht selten gelingt es Hacker:innen die User-Datenbanken größerer Online-Dienste zu erbeuten. Die miteinander verknüpfen Mail-Adressen und Passwörter probieren sie dann direkt bei anderen Seiten aus, die zwar nicht vom eigentlichen Hack betroffen sind, wo die Anmeldedaten für viele User:innen aber dieselben sind.

## Zufällige Passwörter leicht merken

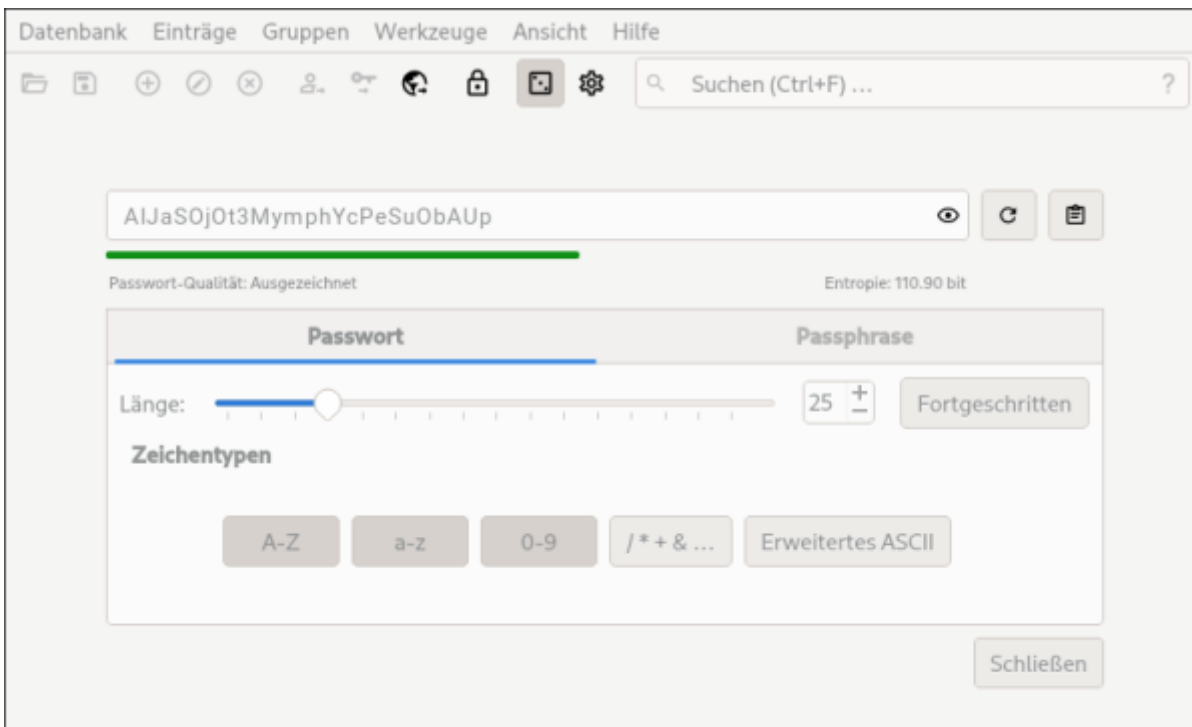
Ein zufällig generiertes Passwort muss nicht immer schwer zu merken sein. Diese beiden Passwörter beispielsweise sind etwa ähnlich „stark“:

KU6D7caw74B4pe7FLXLU

balsamic trailside frantic photo unexposed cloning mutable filler

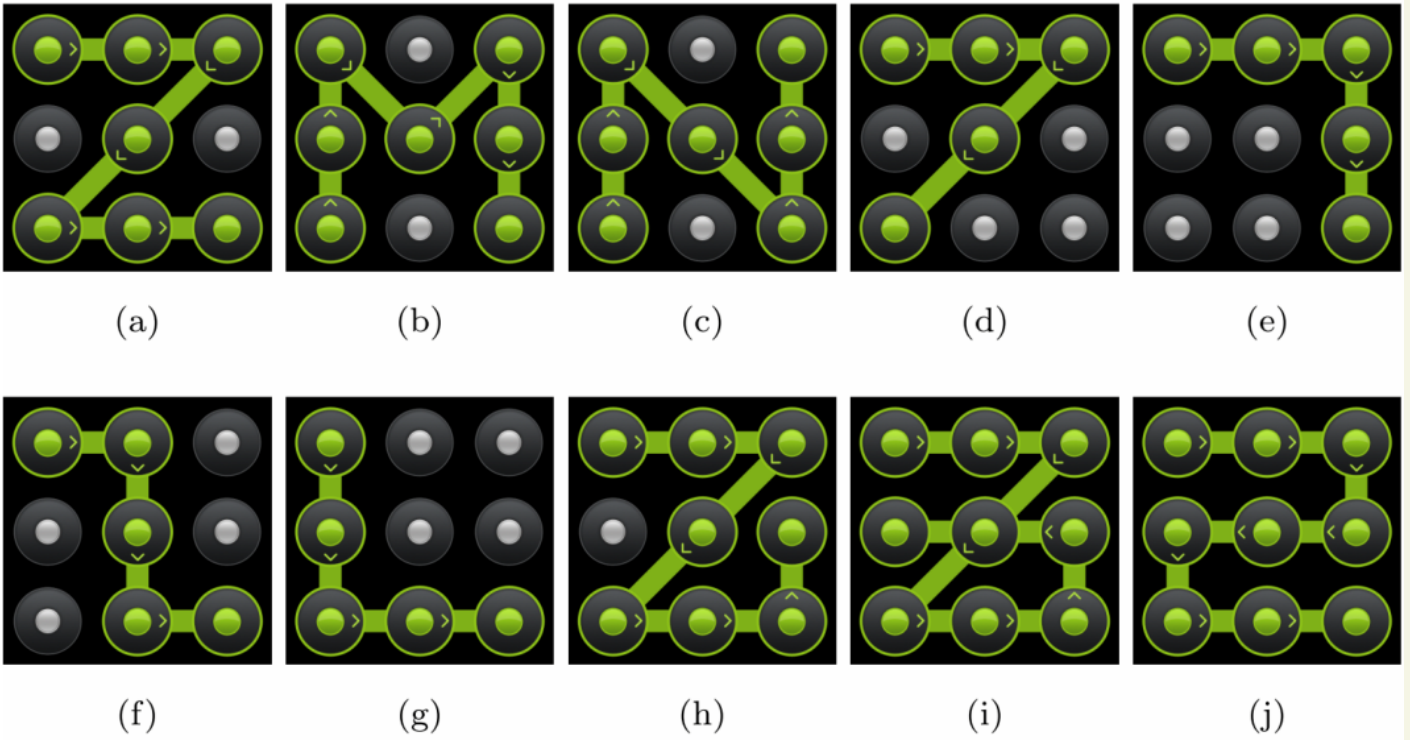
Das erste ist eine zufällige Kombination von Buchstaben und Zahlen. Das zweite ist eine zufällige Aneinanderreihung von 8 Wörtern die aus einer Liste von knapp 8000 Wörtern ausgewürfelt wurde, auch Diceware-Passphrase genannt.

**Diceware-Passphrases sind besonders nützlich für Festplatten-Verschlüsselung oder als Master-Passwort für Passwort-Datenbanken**, also immer man keinen [Passwort-Manager](#) zur Hand hat. Der eingebaute Passwort-Generator (siehe Bild) von [KeePassXC](#) kann auch Diceware-Passphrases erstellen. Falls es dich interessiert, kannst du [hier weiterlesen](#) wie Diceware funktioniert und wieso sie so heißt.



## Displaysperre/Muster

In deinem Handy sind auch Sensible Daten gespeichert. Im besten Fall hat niemand außer dir Zugriff darauf, allerdings kommt auch das auf dein Sperrmuster oder Pin an. Diese Muster sind besonders häufig und können dementsprechend einfach geknackt werden:



**Figure 3: Most Popular Patterns**

Im besten Fall benutzt du lieber einen Pin als ein Muster, wenn dieser Pin dann noch 12 oder mehr Zeichen hat, umso besser.

Version #14

Erstellt: 2024-12-18 17:57:37 UTC von Admin B

Zuletzt aktualisiert: 2025-01-17 10:55:26 UTC von Som31\_3ls3