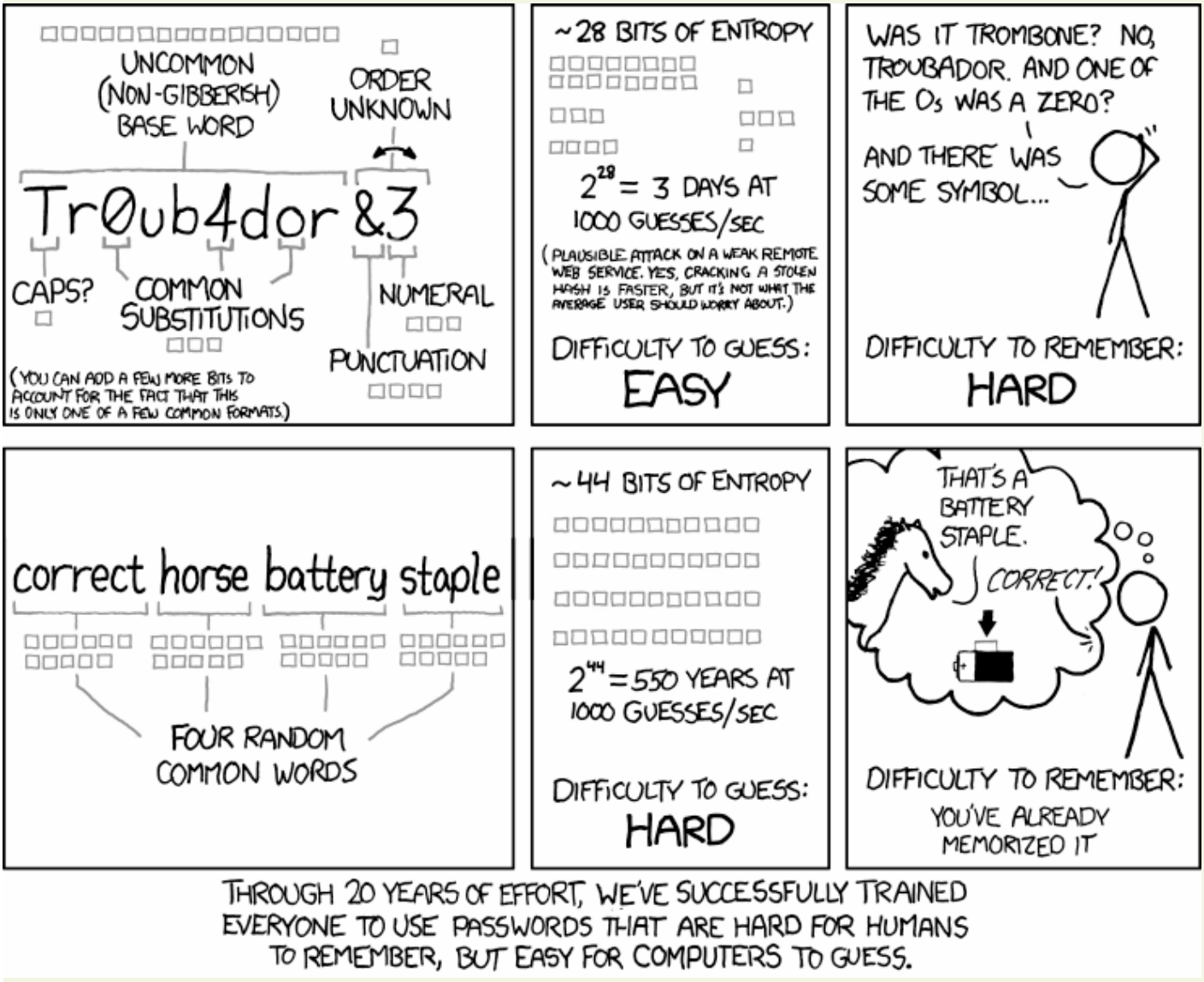
Sichere Passwörter/Muster

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.



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 begrenze 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-Addressen 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.

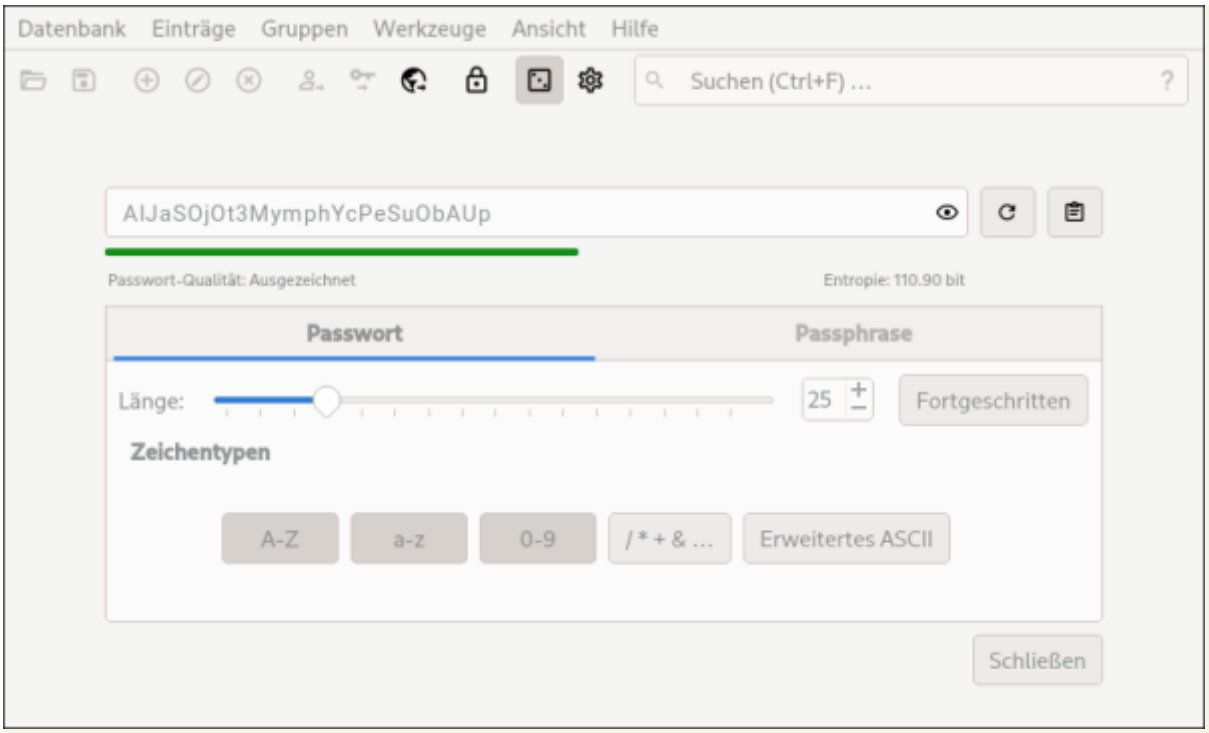
Zufällige Passwörter leicht merken

> 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:

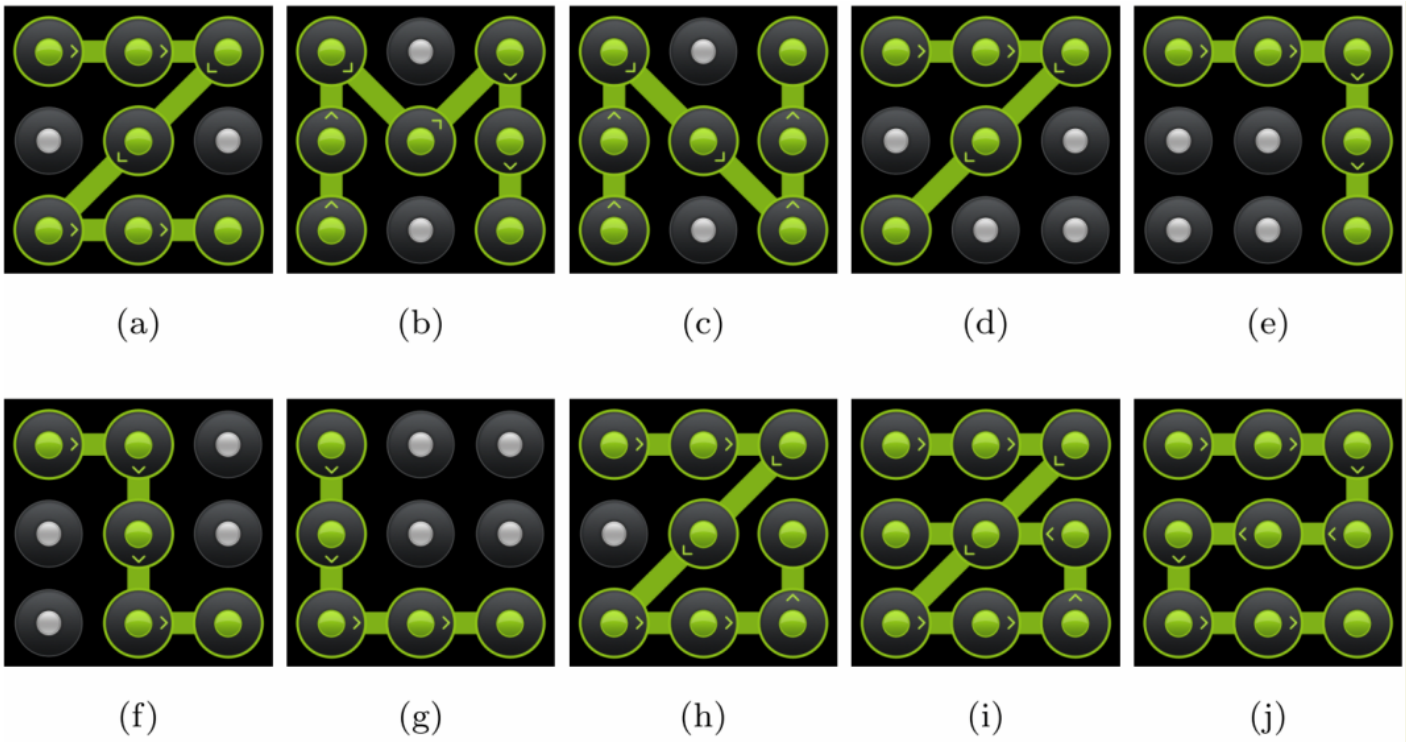


Figure 3: Most Popular Patterns

Im besten Fall benutzt du lieder 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