

# Tutorial / Übung Password Strength

Alphabet  $A = \{a, \dots, z, A, \dots, Z, 0, \dots, 9, \text{SPECIALCHARS}\}$

SPECIALCHARS = [https://www.owasp.org/index.php/Password\\_special\\_characters](https://www.owasp.org/index.php/Password_special_characters)

## Aufgabe 1

Wie viele mögliche Passwörter lassen sich aus  $A$  generieren, wenn  $N$  die Anzahl der Stellen im Passwort ist?

## Aufgabe 2

Wie viele mögliche Passwörter lassen sich aus  $A$  generieren, wenn die Zeichen aus  $A$  nur einmal verwendet werden dürfen (also ohne Wiederholungen?). Die Länge des Passworts ist wiederum  $N$ .

## Aufgabe 3

Nehmen Sie an, dass Sie auf einem Standalone Rechner eine Milliarde Kombinationen pro Sekunde durchtesten können.

Wie lange (Jahre) dauert eine Brute-Force-Attacke eines Passwortes aus Aufgabe 1 mit Zeichenlänge 10?

Wie lange (Jahre) dauert eine Brute-Force-Attacke eines Passwortes aus Aufgabe 2 mit Zeichenlänge 10?

## Aufgabe 4

Warum werden bei Passphrasen minimum 20 Zeichen verlangt?

Inwiefern unterscheidet sich diese Eigenschaft von herkömmlichen Passwörtern?