Berechnung der möglichen Passwortkombinationen

Nachfolgend wird die Anzahl der möglichen Kombinationen eines Passwortes für das Programm „Chess Online“ berechnet. Die Berechnung bezieht sich dabei auf die ungünstigste Wahl mit der Passwortlänge von 10 Zeichen. Es wurde sich auf die schlechteste Wahl beschränkt, da die mathematische Sicherheit der schlechtesten Wahl auch die mathematische Sicherheit aller anderen Längen bestätigt.

Anmerkung: Bei der untenstehenden Berechnung wird ein 4-stelliger Code stellvertretend für die Verteilungen der Zeichensätze auf die zehn Stellen verwendet. Die Codes haben dabei die Form ***K-G-Z-S***, wobei die Buchstaben wie folgend übersetzt werden:

K = Kleinbuchstaben G = Großbuchstaben

Z = Ziffern S = Sonderzeichen

Beispiel: 2-3-2-3

- ⇨ Passwort aus zwei Kleinbuchstaben, drei Großbuchstaben, zwei Ziffern und 3 Sonderzeichen

Zur Erleichterung der Berechnung werden die möglichen Aufteilungen in zwei Kategorien aufgeteilt. Da aufgrund der Passwortrestriktion, dass jeder Zeichensatz an mindestens zwei Stellen vertreten sein muss, nur zwei Stellen frei wählbar sind, teilen sich die Aufteilungen in Codes, welche die frei wählbaren Zeichen dem gleichen Zeichensatz zuordnen und denen, welche die freien Stellen unterschiedlichen Zeichensätzen zuordnen.

Zur Berechnung der möglichen Variationen eines Code wurde folgende allgemeine Formel benutzt, wobei die Variablen die Anzahl der Zeichen des jeweiligen Zeichensatzes angeben:

$$\binom{10}{k} * 26^k * \binom{10-k}{g} * 26^g * \binom{10-k-g}{z} * 10^z * 8^s$$

Kategorie 1: Frei wählbare Zeichen sind nicht Teil des gleichen Zeichensatzes

Codes:	3-2-2-3 3-2-3-2 3-3-2-2 2-3-2-3 2-3-3-2 2-2-3-3
Rechenterme:	
$\binom{10}{3} * 26^3 * \binom{7}{2} * 26^2 * \binom{5}{2} * 10^2 * 8^3$	
$\binom{10}{3} * 26^3 * \binom{7}{2} * 26^2 * \binom{5}{3} * 10^3 * 8^2$	
$\binom{10}{3} * 26^3 * \binom{7}{3} * 26^3 * \binom{4}{2} * 10^2 * 8^2$	
$\binom{10}{2} * 26^2 * \binom{8}{3} * 26^3 * \binom{5}{2} * 10^2 * 8^3$	
$\binom{10}{2} * 26^2 * \binom{8}{3} * 26^3 * \binom{5}{3} * 10^3 * 8^2$	
$\binom{10}{2} * 26^2 * \binom{8}{2} * 26^2 * \binom{6}{3} * 10^3 * 8^3$	
Berechnung der Gesamtsumme:	
3-2-2-3	15.329.826.570.000.000
3-2-3-2	19.162.283.210.000.000
3-3-2-2	49.821.936.350.000.000
2-3-2-3	15.329.826.570.000.000
2-3-3-2	19.162.283.210.000.000
2-2-3-3	5.896.087.142.000.000
Gesamtsumme	**124.702.243.052.000.000**

Kategorie 2: Frei wählbare Zeichen sind Teil des gleichen Zeichensatzes

Codes:	4-2-2-2 2-4-2-2 2-2-4-2 2-2-2-4
Rechenterme:	
$\binom{10}{4} * 26^4 * \binom{6}{2} * 26^2 * \binom{4}{2} * 10^2 * 8^2$	
$\binom{10}{2} * 26^2 * \binom{8}{4} * 26^4 * \binom{4}{2} * 10^2 * 8^2$	
$\binom{10}{2} * 26^2 * \binom{8}{2} * 26^2 * \binom{6}{4} * 10^4 * 8^2$	
$\binom{10}{2} * 26^2 * \binom{8}{2} * 26^2 * \binom{6}{2} * 10^2 * 8^4$	
Berechnung der Gesamtsumme:	
4-2-2-2	37.366.452.260.000.000
2-4-2-2	37.366.452.260.000.000
2-2-4-2	5.527.581.696.000.000
2-2-2-4	3.537.652.285.000.000
Gesamtsumme	**83.798.138.501.000.000**

Bilden der Summe aller möglichen Kombinationen durch Addieren Ergebnisse der beiden Kategorien

Kategorie 1	124.702.243.052.000.000
Kategorie 2	83.798.138.501.000.000
Gesamtsumme	**208.500.381.553.000.000**

Ergebnis: Es gibt insgesamt *208.500.381.553.000.000 Möglichkeiten* für ein Passwort mit jeweils zwei Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen, wenn das Passwort eine Länge von zehn Zeichen hat!

Fallbeispiel 1: Brute-Force-Dauer bei 30,45 Passwörtern pro Sekunde

Für das erste Fallbeispiel wird die ungefähre Dauer eines Brute-Force-Angriffs ausgerechnet, wenn man davon ausgeht, dass der Angreifer 30,45 Passwörter pro Sekunde schafft (siehe 3.2). Hierbei wird vom Worst-Case, also dass alle Passwörter überprüft werden müssen, ausgegangen.

in Sekunden (/30.45)	6.847.303.171.000.00
in Minuten (/60)	144.121.719.500.000
in Stunden (/60)	1.902.028.659.000
in Tagen (/24)	79.251.194.110
in Jahren (/365.25)	216.977.944

Fallbeispiel 2: Brute-Force-Dauer bei 50.000.000 Passwörtern pro Sekunde

Beim zweiten Fallbeispiel wird die Anzahl der Passwörter pro Sekunde auf 50.000.000 erhöht. Es wird wieder davon ausgegangen, dass alle Passwörter überprüft werden müssen.

in Sekunden (/50.000.000)	4.170.007.631
in Minuten (/60)	69.500.127
in Stunden (/60)	1.158.335
in Tagen (/24)	48.264
in Jahren (/365.25)	132