Hoher Laufzeitaufwand als Schutz vor Entschlüsselung durch systematisches Ausprobieren aller Möglichkeiten /Brute-Force

Definition Brute-Force

Die Brute-Force-Methode bzw. Methode der rohen Gewalt, auch Exhaustionsmethode (von lat. *exhaurire* = ausschöpfen), ist eine Lösungsmethode die auf dem Ausprobieren aller möglichen Fälle beruht.

Aus der Definition folgt nun, dass ein Passwort um so sicherer ist, je mehr Kombinationsmöglichkeiten durch verschiedene Zeichen möglich sind und natürlich, je länger es ist.

Kombinationen = Zeichenanzahl $^{\text{Passwortlänge}}$

Beispiele:

Alphabet bestehend aus Kleinbuchstaben mit 26 verschiedenen Zeichen, die Passwortlänge sei 7:

26^7 = **8.031.810.176 Möglichkeiten**

wenn das Passwort nur einen Buchstaben länger ist:
26^8 = **208.827.064.576 Möglichkeiten**

==> pro Verlängerung des Passwortes um 1 Zeichen, steigert sich die Anzahl der Möglichkeiten um ein 26 faches!

Alphabet bestehend aus Groß- und Kleinbuchstaben sowie Zahlen

62 verschiedene Zeichen sind enthalten. Bei einem 7 stelligen Passwort würde der schnellste Einzelrechner der Welt maximal 28 Minuten brauchen.

Bei einem 15 stelligen Passwort hingegen schon 11.631.483.456 Jahre.

--> Je mehr Zeichen in einem Passwort möglich sind und je länger dieses ist desto sicherer ist es auch, jedoch lässt sich ein Zufallstreffer, möglicherweise schon beim 4259 Versuch nicht ausschließen.