**Beispiel 1**

Passwort mit 7 Zeichen, nur Kleinbuchstaben

* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛=26^7
* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛=26∗26∗26∗26∗26∗26∗26
* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛= 8.031.810.176

Beispiel 2

Passwort mit 8 Zeichen, Kleinbuchstaben, Großbuchstaben und Ziffern, z.B.: „9P1auL82“

* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛=(26+26+10) 8=62 8
* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛= 218.340.105.584.896,𝑎𝑙𝑠𝑜 𝑐𝑎.218∗10 12=218 𝐵𝑖𝑙𝑙𝑖𝑜𝑛𝑒𝑛

**Beispiel 3**

Zum Vergleich: Passwort mit 48 Zeichen, nur BINÄR, also z.B.: „0101001010110110100110110101111101110010100101001“

* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛=2 48
* 𝐾𝑜𝑚𝑏𝑖𝑛𝑎𝑡𝑖𝑜𝑛𝑒𝑛= 281.474.976.710.656,𝑎𝑙𝑠𝑜 𝑐𝑎.281∗10 12=281 𝐵𝑖𝑙𝑙𝑖𝑜𝑛𝑒𝑛
* FAZIT? Vergleich mit Beispiel 2?

Aufgaben

**Berechnen Sie:**

1. **Wie lange dauert es maximal, das Passwort im ersten Beispiel zu knacken?**

Nehmen wir an, ein Angreifer kann 1 Milliarde Passwörter pro Sekunde überprüfen.

8.031.810.176/1.000.000.000 p/sec = 8s

1. **Wie lange dauert das Knacken des Passworts im Beispiel 2 maximal?**

1 Milliarde Passwörter pro Sekunde (angenommen)

218.340.105.584.896/1.000.000.000 p/sec = 218s

1. **Das waren die maximalen Knack-Zeiten. Wie lange dauert durchschnittlich jeweils, die beiden Passwörter zu knacken?**

Durchschnittlich muss der Angreifer die Hälfte der Kombinationen ausprobieren, bevor er das richtige Passwort findet. Mit derselben Annahme 4 Sekunden beim ersten und 109 Sekunden beim zweiten.

**Es gilt der generelle Hinweis, dass ein gutes Passwort 8 Zeichen lang sein soll. Berechnen Sie die Kombinationsmöglichkeiten und daraus die durchschnittliche „Passwortknackdauer“ in folgenden Fällen:**

1. **Wenn nur Zahlen genutzt werden**

100.000.000/1.000.000.000 = 0,1 s

1. **Wenn Groß- und Kleinbuchstaben genutzt werden (ohne Umlaute)**

5.3459729e+13/1.000.000.000 = 53459,72h

1. **Wenn Groß- und Kleinbuchstaben, Zahlen und die typischen 21 Sonderzeichen genutzt werden.**

2.2522922e+15/1.000.000.000 = 2252292.23h

**Wir betrachten nun ein Passwort von 10 Zeichen, das nur Groß- und Kleinbuchstaben enthält im Vergleich zum Passwort aus Aufgabe 2c). Fragen dazu:**

**a. Schätzen Sie zunächst „aus dem Bauch heraus“ ab welches besser ist!**

2c ist besser, weil es schwerer ist zu knacken.

**b. Und nun bitte die Kombinationsmöglichkeiten ausrechnen und vergleichen!**

144.555.105.949.057.024

**c. Überrascht? Bitte ein Fazit!**  
 Nicht wirklich, macht ja Sinn, dass es schwerer ist, je nach Länge.

**Die Güte eines Passworts lässt sich auch als sogenannte Informationsdichte („Entropie“) in „Bit“ ausdrücken:**

**a. Wieviel Bit Verschlüsselungstiefe entsprechen die Kennwörter der Aufgaben 2a und 2c? (Bitte über den Log2(x) ausrechnen oder mit 2^x ausprobieren). Anmerkung: Log2(x)=Log10(x)/Log10(2) hilft, wenn der Log2(x) fehlt!**

Für 2a: 26,57

Für 2c: 51

**b. Vergleichen Sie das mit einer heute „üblichen“ Verschlüsselungstiefe von 128 bit! Bitte kommentieren!**

Natürlich ist das deutlich mehr.

**Wie vielen Hex-Ziffern entspricht das Passwort aus Bsp. 3? HEX kennen Sie aus SuD!**

13 0-F

**Warum machen Anbieter von Onlinediensten technische Vorgaben für die verwendbaren bzw. zu verwendenden Zeichen und schließen zum Teil Umlaute aus?**

Um sicher zu stellen, dass die Passwörter noch schwerer bis zu gar nicht zu knacken sind und mit allen anderen Vorgängen wie z.B. Hashing oder Datenbanken Kompatibel sind und nicht zu Problemen führen.