**ITG 18.06.2024**

**Aufgaben**

1. Wenn sie die „Kombinationsmöglichkeiten“ schon ausgerechnet haben: Wie war dann die Formel für die Berechnung dieser vergleichbaren "Bitlänge"?  
   Bitlänge=log2​(N^L)

Bitlänge=L⋅log2​(N)

1. Wie viel Bit entspricht ein Hexadezimales Passwort von 8 Stellen, also z.B. 3e48b39a?  
   32 Bit
2. Schätzen Sie bitte die **Komplexität in Bit** der folgenden Passwörter ab:  
   **/3%$6H\* :: Bit 39  
   68421789615423 :: Bit 47  
   uZtbLnvGfEbFvH :: Bit 80  
   buchstabensuppenkartoffelgemuesebrei :: Bit 160**
3. Welches der Kennwörter können Sie sich am besten merken?  
   buchstabensuppenkartoffelgemuesebrei
4. Gehen Sie auf die folgende Seite und prüfen Sie, ob sich in etwa richtig lagen! <https://wiesicheristmeinpasswort.de/>  
   Dort ist die **Infomationsdichte** etwas ungeschickt mit Dezimalpunkt und drei Nachkommastellen angegeben, aber ansonsten ist das eine gut gemachte Seite.  
     
   Falsch eingeschätzt habe ich: das letzte
5. Schauen Sie sich die beiden Passwörter **Paul1982** und **9P1auL82** an.
   1. Worin besteht der Unterschied?

Es ist komplexer die zahlen sind anders verteit

* 1. Wie wirkt sich das auf die **Kombinationsmöglichkeiten** aus?

Schon stark, da im Wörterbuch kein P1aul so steht

* 1. Wie wirkt sich das auf die **Entropie** aus?

gesundheit

* 1. Checken Sie die beiden auf der o.g. Website!

Sehr starke auswirkung

* 1. **Sie sollten jetzt überrascht sein…** Bitte ein Fazit!

Nicht wirklich

# ZUSATZAUFGABE

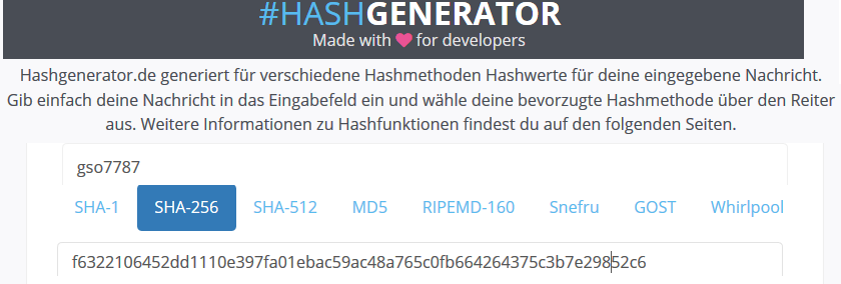
Aus: <https://www.dr-datenschutz.de/hashwerte-und-hashfunktionen-einfach-erklaert/>

**Speichern von Passwörtern**

Passwörter sollen verschlüsselt gespeichert werden, damit bei einem Angriff diese nicht im Klartext gelesen werden können. Aber wie können die Passwörter genutzt werden, wenn diese „verschlüsselt“ gespeichert sind? Die Passwörter werden mittels einer Hashfunktion in Hashwerte umgewandelt – nur diese Hashwerte werden gespeichert (nicht die Passwörter selbst). Gibt ein Nutzer bei einer [Authentisierung](https://www.dr-datenschutz.de/authentisierung-authentifizierung-und-autorisierung/) sein Passwort ein, wird bei der Eingabe wieder mit derselben Hashfunktion der Hashwert berechnet und mit dem gespeicherten Hashwert verglichen. Bei Übereinstimmung gilt der Benutzer als authentifiziert.

Und hier der Hash-Generator zum Ausprobieren und Verstehen:

<https://www.hashgenerator.de/>



1. Nennen Sie eine Anwendung, bei der Sie schon mit Hashs gearbeitet haben.
2. Warum gibt es unterschiedliche Hash-Verfahren?
3. Wie lang ist ein MD-5 Hash, z.B. „**25d55ad283aa400af464c76d713c07ad**“.
4. Betrachten Sie die Passwörter **Paul1982** und **Paul1928.**
   1. Schätzen Sie: Haben die beiden Passwörter unterschiedliche Hashs?
   2. Warum(nicht)?
   3. Probieren Sie das auf der Webseite aus!
   4. Sie sollten jetzt nicht überrascht sein.
5. Hashs sind nicht notwendigerweise eindeutig, d.h. **es könnte zwei Passwörter** geben, die denselben Hash liefern. Wie wahrscheinlich ist das bei MD5?