Grenzen der Berechenbarkeit

Kennwortknacker ⇔ Wie sicher ist ein Schlüssel?

Es gibt verschiedene Ansätze, wie ein Kennwort „geknackt“ werden kann. Überlegen Sie kurz, welche?

Rufen Sie den „Kennwortknacker“ auf. Hier können Sie ein zu „knackendes“ Kennwort eingeben und dem Programm dabei zusehen, wie es das Kennwort herausfindet. Wenn Sie unter Einstellungen die dafür nötigen Zeichensätze angeben (Sonderzeichen stehen nicht zur Verfügung), wird das Programm dieses Ziel auf jeden Fall erreichen.

*Experimentieren Sie mit dem Programm herum (zunächst mit einem kurzen Kennwort)! Welches Verfahren wird hier benutzt? (Der gängige Fachbegriff dafür ist **Brute-Force**-Verfahren.)*

Aufgabe 1: Stellen Sie in einem Tabellenkalkulationsblatt zusammen, wie lange das Programm bei verschiedenen Einstellungen und verschiedenen Kennwortlängen braucht, um das Kennwort zu ermitteln. Überlegen Sie sich dazu ein systematisches Vorgehen, sodass eine systematische und aussagekräftige Darstellung dabei herauskommt. Lassen Sie sich Ihre Ergebnisse auch als Diagramm anzeigen.

Die Erkenntnisse, die Sie in Aufgabe 1 schöpfen konnten, sind nicht spektakulär, es ging aber hier darum, einen konkreten Eindruck vom sogenannten **Laufzeitverhalten** des Kennwortknackerprogramms zu gewinnen. Die dahinter stehende abstraktere **Frage** ist die, **wie sich** der Aufwand – in unserem Fall der **Zeitaufwand** – für die Abarbeitung des Programms **im Verhältnis** zum ‚Umfang‘ der Datenbasis, auf der das Programm arbeitet, **verändert**.

Ganz offensichtlich steigt die Laufzeit mit zunehmender Länge und ‚Komplexität‘ des Kennworts an. Welche Faktoren spielen (sicherlich) außerdem eine Rolle (auch wenn Sie diese nicht experimentell erfassen konnten/können)?

Aufgabe 2: Wir lassen jetzt die zusätzlichen Faktoren aus der vorangegangenen Überlegung außer Acht und betrachten die Angelegenheit ganz theoretisch: Uns interessieren nur

- die Anzahl der Zeichen des Kennworts,
- die Größe des Zeichensatzes (Anzahl der möglichen/geprüften Zeichen)
- und die Anzahl der Versuche, das richtige Kennwort zu finden (= Anzahl der erzeugten „Probierkennwörter“, bis das richtige gefunden ist).

Stellen Sie eine allgemeine Regel auf, wenn möglich gerne eine Formel, mit der sich das Verhältnis dieser drei Größen zueinander ausdrücken lässt.

Das Kennwortknackerprogramm legt seinem Vorgehen die Länge des zu ermittelnden Kennworts zugrunde. Das ist wenig realistisch: Normalerweise weiß man bei einem unbekannten Kennwort bestenfalls, wie lang es mindestens sein muss. Was würde sich an der in Aufgabe 2 aufgestellten Regel ändern, wenn man mit in Betracht zöge, dass „Probierkennwörter“ verschiedener Länge erzeugt werden müssen?

Aufgabe 3: Nehmen Sie nun alle bisher gewonnenen Erkenntnisse und angestellten Überlegungen als Grundlage, um eine konkrete Antwort auf folgende Frage zu formulieren: Wie sollte ein Kennwort gestaltet sein, damit es

a) für die alltägliche private Nutzung oder
b) für die Nutzung zur Sicherung von Staatsgeheimnissen

als „sicher“ gelten kann. Recherchieren Sie dazu im Internet, wie viele Schlüssel die derzeit schnellsten Computer pro Sekunde testen können. Begründen Sie Ihren Ratschlag. Gerne dürfen Sie dazu auch entsprechende Empfehlungen im Internet zu Rate ziehen – sorgen Sie aber dafür, dass Sie diese (bzw. die Gründe dafür) auch verstanden haben.