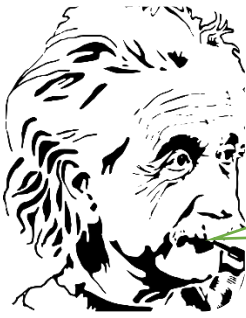


5.3. Sicherheit ist relativ



Wenn die Entwicklung der
Quantencomputer weiter voranschreitet,
sind unsere heutigen
Verschlüsselungsverfahren (z.B. bei
Whatsapp ...) (bald) nicht mehr sicher.

Max und Gloria grübeln über diese Aussage und fragen Max Vater nach Rat. Dieser meint:

„Lange glaubte auch Caesar sein Verfahren sei nicht „knackbar“. Das stellte sich als Irrtum heraus. Schon ein paar Jahre nachdem Caesar das Verfahren entwickelt hatte, gelang es Gelehrten die Caesar-Verschlüsselung zu knacken. Ich habe eine Aufgabe für euch.“

Er übergibt ihnen einen Zettel:

TRIGV UZVD! ELKQV UVE KRX!

Auftrag:

1. Knacke das Verfahren. Finde den passenden Schlüssel.
2. Wie lautet die entschlüsselte Nachricht?
3. Stimmen folgende Aussagen? Kreuze die **richtigen** Aussagen an:
 - ☐ Unsere Daten sind immer sicher, das heißt niemand kann sie jemals „knacken“.
 - ☐ Ich achte darauf welche Daten ich öffentlich zugänglich mache. Es besteht immer die Gefahr, dass meine Daten geknackt werden.
 - ☐ Es gibt kein 100% sicheres Verfahren.
 - ☐ Quantentechnologie könnte in Zukunft ein Problem für die derzeit verwendeten Verfahren werden.