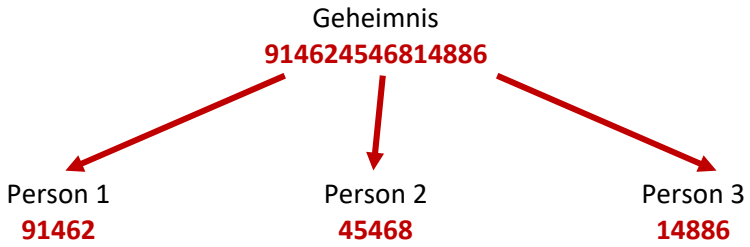
# Geheimnis teilen

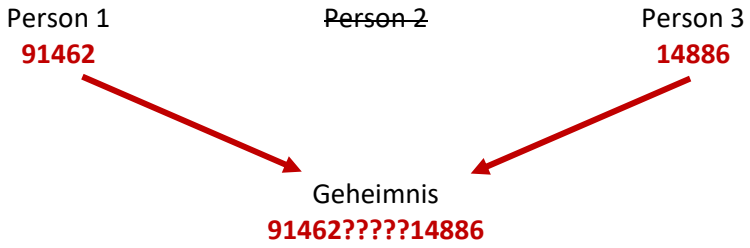
Ab und an werden Geheimnisse geteilt. Und manchmal muss ein Geheimnis sicher geteilt werden. Drei Freundinnen haben zum Beispiel Retrogames gesammelt und lagern diese neu in einem Banksafe. Da keine der Freundinnen alleine über die Sammlung verfügen darf, bitten sie die Bank, den Code für den Banksafe dreizuteilen. Jede der drei Freundinnen erhält von der Bank einen Drittel des gesamten Safecodes und behält diesen Teilcode für sich geheim.

Dank dieser Lösung können die Freundinnen den Safe nur öffnen, wenn sie zu dritt zur Bank gehen und jede Freundin ihren Teilcode verdeckt eingibt.

Ist der Safecode z. B. G = 914624546814886, so bildet die Bank wie folgt drei Teilcodes:




Zwei der drei Freundinnen möchten nun die wertvolle Sammlung verkaufen und den Safe öffnen. Die dritte Kollegin ist nicht einverstanden und weigert sich, ihren Teilcode einzugeben. Wie schwierig ist es für die zwei Freundinnen, den dritten Teilcode zu erraten und an die Sammlung zu gelangen?




Hierzu müssen 5 Ziffern aus dem Zeichensatz 0 bis 9 richtig erraten werden. Das heisst, es gibt 10’000 Möglichkeiten, die man mit Geduld durchprobieren könnte. Man stellt fest: Die Teilgeheimnisse verraten zu viel über das Gesamtgeheimnis. Das Zerschneiden einer Schatzkarte ist aus gleichem Grund nicht sicher, weil jede Teilkarte zu viel über das Versteck und seine Umgebung verrät.

Um ein Geheimnis sicher zu teilen, muss ein anderes Verfahren gefunden werden. Die einzelnen Teilgeheimnisse dürfen dabei nur ganz wenig oder nichts über das Gesamtgeheimnis aussagen.

Da hilft die Mathematik weiter. So sagt der Rest einer Division nichts über Dividend und Divisor aus. Die Division mit Rest wird «Modulo» genannt und in vielen Programmiersprachen mit dem Zeichen «%» dargestellt. Der Rest 7 kann zum Beispiel aus folgenden Divisionen entstehen:

- $11 \,\%\, 4 = 7$
- $23 \,\%\, 16 = 7$
- $1892 \,\%\, 13 = 7$

Es gibt unendlich viele Restdivisionen, aus denen 7 resultiert. Mit dem Trick der Restdivision können Geheimnisse gemäss folgendem Verfahren sicher geteilt werden.

## Verfahren:

1. entscheiden, auf wie viele Personen $m$ das Geheimnis aufgeteilt werden soll.
2. wählen einer grossen Zahl $N$.
3. wählen eines Geheimnisses $G$ zwischen $0$ und der Zahl $N$
4. für alle Personen mit Ausnahme einer Person: eine zufällige Zahl zwischen $0$ und $N$ wählen. Diese Zahlen sind die Teilgeheimnisse $t_1$, $t_2$ bis $t_{m-1}$.
5. Vorgehen für das letzte Teilgeheimnis $t_m$:
   - die Summe $\Sigma$ aller Teilgeheimnisse $t_1$ bis $t_{m-1}$ bilden: $\Sigma = \sum_{k=1}^{m-1} t_k$
   - Rest $R$ bei der Restdivision von $\Sigma$ Modulo $N$ berechnen: $R = \Sigma \,\%\, n$
   - die Differenz $D$ vom Geheimnis $G$ – Rest $R$ berechnen: $D = G - R$
   - falls $D$ eine positive Zahl ist, so wird $t_m$ zu $D$,
     sonst wird $t_m$ zu $D + N$
6. das Geheimnis $G$ lässt sich aus der Summe $\Sigma$ aller Teilgeheimnisse Modulo $N$ berechnen

## Beispiel:

Wir wählen $N = 23$ und als Geheimnis $G = 11$, welches auf vier Personen aufgeteilt werden soll. Die zufälligen Zahlen für die ersten drei Personen wählen wir mit $7$, $13$ und $19$. Die Summe $\Sigma$ der ersten drei Geheimnisse beträgt $39$. Diese Summe $\Sigma$ Modulo $N$ rechnen: $R = 39 \,\%\, 23 = 16$. Die Differenz $D = G - R = 11 - 16 = -5$ ist negativ. Daher wird $N$ zu $D$ addiert: $t_4 = -5 + 23 = 18$. Das vierte Geheimnis ist folglich $18$.

**Aufgabe 1:**

Kontrollieren Sie mit Schritt 6 des Verfahrens, ob $G$ aus den vier Teilgeheimissen aus obigem Beispiel korrekt errechnet werden kann.

.....

.....

**Aufgabe 2:**

Wenden Sie das Verfahren ab Schritt 4 für $N = 53$ und das Geheimnis $G = 23$ an.
Generieren Sie dabei vier Teilgeheimnisse.

.....

.....

.....

.....

Wenn man das Geheimnis nun knacken will, obwohl sich jemand weigert, sein Teilgeheimnis preiszugeben, müsste man für das fehlende Teilgeheimnis alle Zahlen zwischen $0$ und $N$ durchprobieren. Besonders sicher wird das Teilen von Geheimnissen, wenn $N$ möglichst gross gewählt wird. Die folgende Simulation lässt grosse Geheimzahlen auf bis zu zehn Personen verteilen: http://media.kswillisau.ch/in/cryptShare/index.html.

**Aufgabe 3:**

Generieren Sie mit der Simulation Teilgeheimnisse und versuchen Sie deren Korrektheit mit Hilfe von Taschenrechner, Tabellenkalkulation oder Online-Rechnern zu prüfen.

Beim Teilen von Geheimnissen braucht es in jedem Fall eine vertrauenswürdige Institution, die für die Beteiligten das Geheimnis teilt.