

## Was du in diesen Arbeitsblättern lernst

Ein „Algorithmus“ ist nichts anderes als eine Schritt-für-Schritt Anleitung für den Computer, wie er etwas machen muss, damit etwas Bestimmtes dabei herauskommt.

Algorithmen in den Computer zu programmieren, ist die Aufgabe eines „Programmierers“, und ein Teil der Aufgaben die „Informatiker“ erledigen.

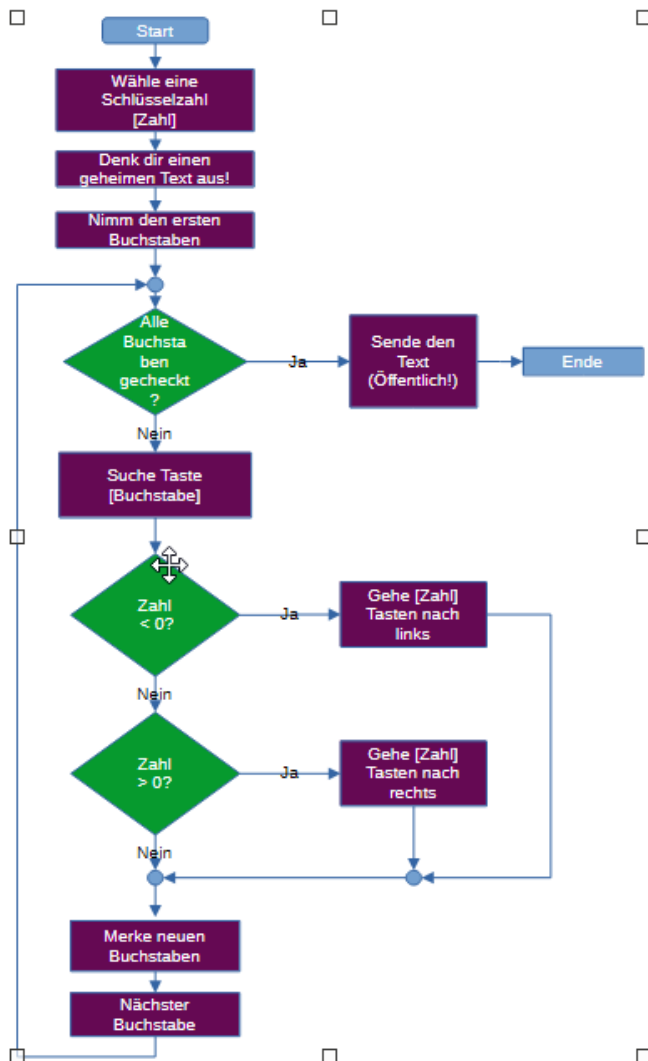
Um Algorithmen aufzuschreiben und (im Kopf oder mit Bleistift und Papier) zu testen eignen sich Flussdiagramme.

Viele Algorithmen bestehen aus sich wiederholenden Anweisungen, die immer wieder ausgeführt werden, solange eine Bedingung erfüllt ist. Man nennt solche Konstruktionen eine "Schleife".

## Verschlüsselung mit der PC Tastatur

Durch Verschlüsselung wird eine geheime Botschaft (eine Nachricht) abhörsicher übermittelt. Die ursprüngliche, lesbare Nachricht nennt man "Klartext". Aus dem Klartext wird durch "Verschlüsselung" mit einem "Schlüssel" ein "verschlüsselter Text" gemacht.

Zuerst das Flussdiagramm.



Dann erkläre ich dir den Algorithmus in Worten:

- 1.) Wähle eine **Zahl** als "Verschlüsselungs-Schlüssel". Sie kann negativ oder positiv sein. Negativ bedeutet "nach links", positiv bedeutet "nach rechts". Wir nehmen als Beispiel +2, also "zwei Tasten nach rechts".
- 2.) Schicke dem Empfänger den Entschlüsselungs-Schlüssel auf einem sicheren Weg (z.B. als SMS mit dem Handy). Da bei diesem Algorithmus der Schlüssel zum Entschlüsseln genau das Gegenteil von dem Verschlüsselungs-Schlüssel ist, muss der Empfänger nur das Vorzeichen umkehren. Aus "+2" wird so "-2".
- 3.) Verschlüsse deine Nachricht. Schreibe den Klartext ab, aber drücke dazu auf der PC Tastatur die Taste, die um **Zahl** neben der richtigen Taste liegt. Erinnerung: **-Zahl** bedeutet, dass du nach links zählen musst, **+Zahl** bedeutet, dass du nach rechts zählen musst. Nehmen wir zum Beispiel an, dein Schlüssel ist +2, und dein Text beginnt mit einem "F"



Dann ist der erste Buchstabe des verschlüsselten Textes 2 nach rechts von F, also H.

Bei dieser einfachen Verschlüsselung ist der Schlüssel zum Entschlüsseln das Gegenteil vom Verschlüsselungs-Schlüssel. Dein Verschlüsselungs-Schlüssel war +2, also ist sein Entschlüsselungs-Schlüssel -2. Der Empfänger bekommt also ein H, und wendet nun seinen Entschlüsselungs-Schlüssel an:



Bei ihm steht jetzt also wieder ein "F". Entschlüsselung gelungen.

4.) Einen Spezialfall haben wir noch: Wenn du beim Tasten zählen über den Rand der Tastatur hinauskommst, zählst du einfach am gegenüberliegenden Ende der Tastenreihe weiter. "P" +2 verschlüsselt ergibt also "Q".



Also: um vom Klartext zum verschlüsselten Text zu kommen, habe ich immer zwei Tasten nach rechts gezählt (+), um den verschlüsselten Text wieder zu entschlüsseln, habe ich den Schlüssel einfach umgedreht, also zwei nach links (-2).

Hier kommt ein komplettes Beispiel:

Klartext	Schlüssel	Verschlüsselter Text
Frohe Schüler lachen gerne	+2	Hzükt Fbkqätz ädbkt, jtz,t

Den Schlüssel übergibt man dem Empfänger auf einem sicheren, geheimen Weg. Der kann den Schlüssel umkehren und aus dem „verschlüsselten Text“ wieder den Klartext gewinnen.

Verschlüsselter Text	Ent-Schlüssel	Klartext
Hzükt Fbkqätz ädbkt, jtz,t	-2	Frohe Schüler lachen gerne

Danach kann man dem Empfänger viele Texte schicken, die man mit diesem geheimen Schlüssel verschlüsselt hat. Der Empfänger kann sie wieder in Klartext verwandeln und lesen.

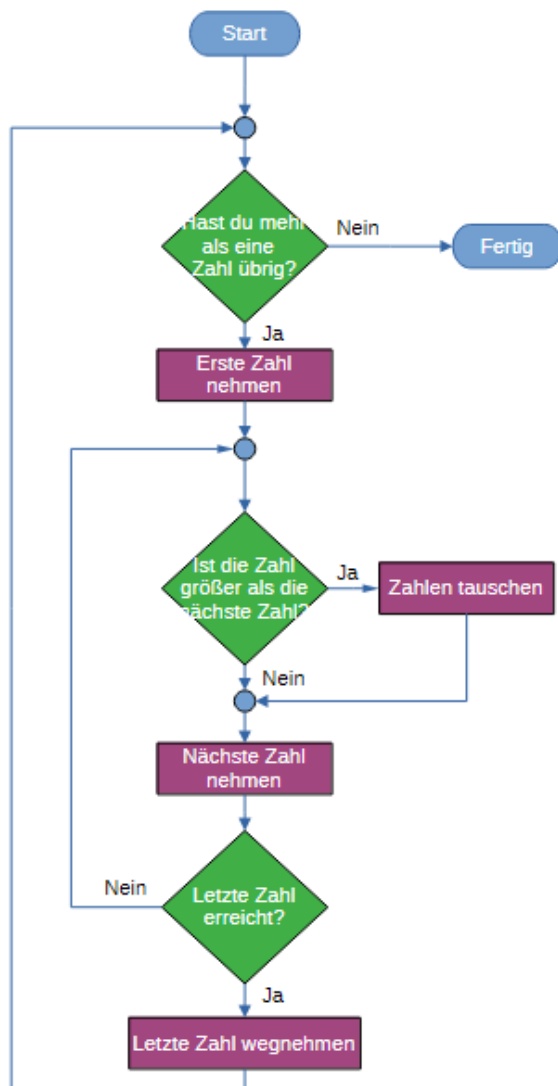
Ein Hacker, der den verschlüsselten Text irgendwie in die Hände kommt hat den Schlüssel nicht, und kann daher die Nachricht nicht in Klartext zurückverwandeln.

### Ein „richtiger“ Algorithmus für den Computer

Eine ganz häufige Computeraufgabe ist „Sortieren“. Es gibt immer etwas zu sortieren. Chats sind zum Beispiel nach Datum und Uhrzeit sortiert (die älteren Beiträge stehen weiter oben in einer Liste). Kontakte sind nach dem Alphabet sortiert (A oben, dann B,C,D ... bis Z). Jetzt kommt ein einfacher Algorithmus (er heißt übrigens „Bubblesort“) der zeigt, wie man mit dem Computer etwas sortieren kann.

Nimm dir ein paar Zettel mit beliebigen Zahlen und probiere es einfach aus. Du wirst sehen, es funktioniert.

Das Flussdiagramm:



Du legst die Zettel mit Zahlen einfach mal irgendwie in einer Reihe hin. Es entsteht eine zufällige Liste von Zahlen.

Jetzt der Algorithmus in Worten:

- Gehe durch die Liste aller Zahlen durch, und vergleiche immer einen Zettel mit dem Zettel, der danach kommt.
- Wenn die Zahl größer ist als die auf dem nächsten Zettel tauschst du die beiden Zettel.
- Wenn du das Ende der Liste erreichst, markiere den letzten Zettel als „erledigt“. Danach beginne wieder von vorne.
- Das wiederholst du so lange bis du alle Zettel „erledigt“ hast.

Wenn du jetzt die Zettel anschaut, sind die Zahlen aufsteigend sortiert.