



Informatik Challenge

Cäsar-Verschlüsselung

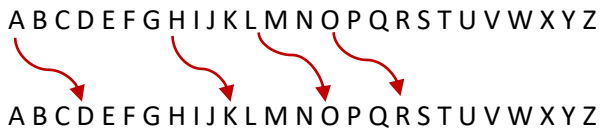
Damit du eine geheime Botschaft an Verbündete weitergeben kannst, ohne dass es der Feind auch versteht, brauchst du einen Code. So einen Code hat Julius Cäsar, ein römischer Feldherr, vor über 2000 Jahren entwickelt. Der Code ist ganz einfach, und darum wird er heute auch nicht mehr für wichtige Botschaften gebraucht.



Julius Cäsar

1 Findest du selbst heraus, was «KDOOR» heissen könnte, und wie der Code funktioniert?

Um eine Botschaft zu entschlüsseln wird der Buchstabe, welcher 3 Schritte weiter im Alphabet ist, gebraucht. Das sieht dann so aus:



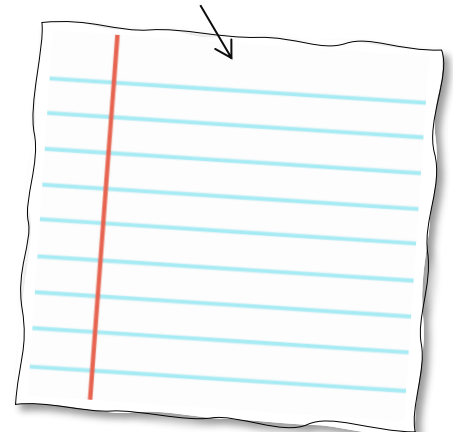
Also würde «HALLO» nun «KDOOR» heissen.

2 Kannst du diese Botschaft entschlüsseln?

ZHOFKHU EXV NDQQ QLFKW IDKUHQ?
GHU JOREXV

Die Lösung ist unten auf dieser Seite.

Hier kannst du die entschlüsselte Botschaft notieren

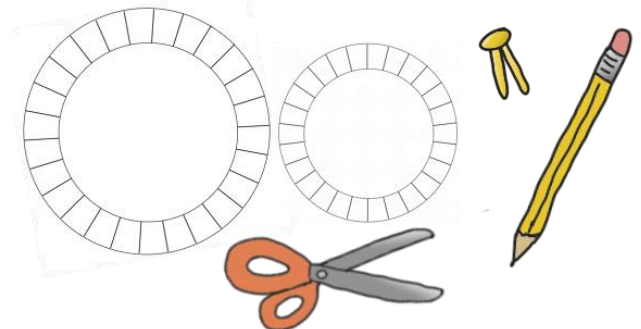


War es einfach, die Botschaft zu entschlüsseln, oder war es eher mühsam?

Um das Verschlüsseln und Entziffern einfacher und schneller zu machen hat Leon Battista Alberti die Chiffrierscheibe entworfen. Da die zwei Scheiben einfach weitergedreht werden können, kann der Code auch verändert werden. Der Empfänger muss aber wissen, um wie viele Buchstaben es verschoben wurde.

3 Um die Chiffrierscheibe zu basteln, brauchst du:

- Kreisvorlage
- Eine Rundkopfklammer
- Eine Schere
- Eventuell einen Stift



Welcher Bus kann nicht fahren?
Der Globus



Schneide die zwei Kreise aus. Eventuell musst du noch das Alphabet drauf schreiben, in jedem Kästchen ein Buchstabe.

Nun befestige die Kreise in der Mitte mit einer Rundkopfklemme, sodass nun bei beiden das Alphabet sichtbar ist.

In dem du den Kreis in der Mitte verschiebst kannst du Botschaften verschlüsseln und entziffern. Achtung: In welche Richtung musst du den Kreis drehen zum Verschlüsseln? Und zum Entziffern?

Cäsar hat das Alphabet jeweils um 3 Schritte verschoben (wie im Bild oben), aber mit der Chiffrierscheibe kannst du verschieben, wie du möchtest, nur musst du noch irgendwie deinem Empfänger kommunizieren, um wie viele Schritte er die Scheibe drehen muss zum Entschlüsseln, sonst kann er die Botschaft nicht verstehen.

4

Hier siehst du nochmals eine verschlüsselte Botschaft. Um wie viele Buchstaben musst du das Rad drehen? Findest du heraus, was da steht?

C 2

YCTWO UWOOGP DKGPGP?

YGKN UKG FGP VGZV PKEJV

MGPPGP

Die Lösung ist unten auf dieser Seite.

Du kannst nun auch eigene Botschaften verschlüsseln und mit deinen Freunden austauschen. So kann niemand eure geheimen Nachrichten lesen!

Viel Spass beim Verschlüsseln und Entziffern!

Informatik Hintergrund: Gemäss dem römischen Schriftsteller Sueton hat Gaius Julius Cäsar mit dieser Methode mit dem Militär kommuniziert. Er verschob das Alphabet jeweils um 3 Buchstaben. Auch der Kaiser Augustus benutzte anscheinend diese Methode, wobei er nur mit einer Verschiebung gearbeitet hat. Als Leon Battista Alberti die Chiffrierscheibe entwickelte, wurde dieser Code viel einfacher umzusetzen. Heute wird der Code nicht mehr verwendet, da er sehr einfach geknackt werden kann (zum Beispiel mit einer Häufigkeitsanalyse).

Impressum: Die MIA-Scouts Informatikaufgaben wurde im Rahmen des Projektes MIA-Scouts der Pädagogischen Hochschule Schaffhausen ausgearbeitet. Die MIA-Scouts werden finanziell unterstützt durch das Programm P-8 von swissUniversities «Stärkung von Digital Skills in der Lehre».

Warum summen Bienen?
Weil sie den Text nicht kennen