MINT Osterquiz

110 + 10100 = 11010

09.04.2020

Aufgabe 7

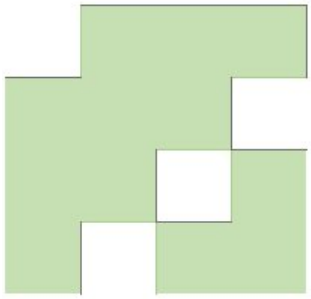
Die geheimen Botschaften des Osterhasen

Absolute Geheimhaltung seiner Existenz hat für den Osterhasen oberste Priorität – das weiß jeder!

Nur wenige wissen jedoch, dass der Osterhase auch einige Aushilfshasen hat, die ihm beim Verteilen seiner Ostereier helfen. Sonst würde er die ganzen Lieferungen auch gar nicht schaffen. Aber damit ihm auch keiner auf die Schliche kommt, müssen die ganzen Nachrichten, die er mit den anderen Hasen austauscht, verschlüsselt werden.

<u>Dafür hat er sich folgende Methode überlegt:</u>

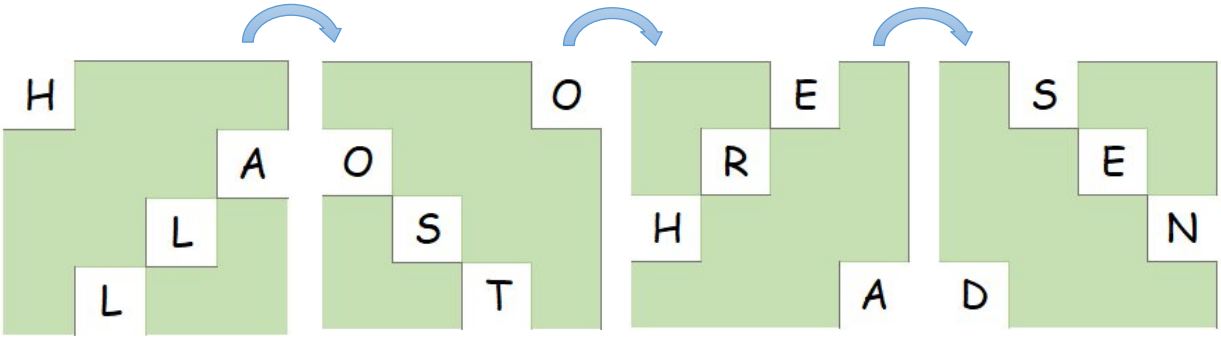
Jeder seiner Hasen bekommt eine geheime Schablone, mit der er seine Nachrichten verschlüsseln und auch entziffern kann. Die Schablone wird auf ein Stück Papier gelegt und von oben nach unten und links nach rechts mit den Buchstaben einer Nachricht ausgefüllt. Danach wird die Schablone einmal im Uhrzeigersinn um 90° gedreht und wieder ausgefüllt.
Nach viermal ausfüllen ist ein Quadrat voll und die Schablone wird auf die nächste Position geschoben.



Eine Beispielschablone

Die Nachricht *"Hallo Osterhasen, die Eier sind fertig!"* würde dann so aussehen:

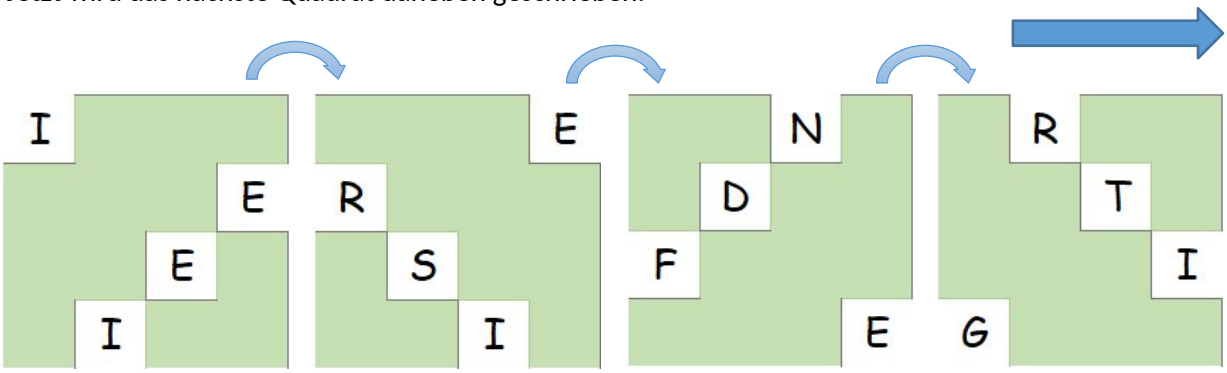
Das erste Quadrat:



Damit ist das erste Quadrat voll:

H	S	E	O
O	R	E	A
H	S	L	N
D	L	T	A

Jetzt wird das nächste Quadrat daneben geschrieben:



Und damit beide Quadrate nebeneinander:

H S E O I R N E
O R E A R D T E
H S L N F S E I
D L T A G I I E

Das war natürlich nicht die echte Schablone des Osterhasen und seiner Helfer…

Aber wir haben eine Nachricht von ihnen abgefangen!

A R E O T L E T K R S E M N G E
H R S A I E E R M O S C D M R E
T N A O N O T R T H I E S K A E
K E T S S F N Z O E I T O I N N

Jetzt darfst du ein wenig knobeln: Könnt ihr die geheime Schablone des Osterhasen erraten und die Nachricht entziffern?

Zwei Tipps:

- Wo macht es Sinn, die Löcher in der Schablone zu platzieren? Nur bei bestimmten Positionen erscheinen beim Schreiben bei jeder Drehung nur freie Felder bis das Quadrat voll ist.
- Manche seltenen Buchstaben treten nur vor oder nach bestimmten anderen Buchstaben auf. Das kann Dir Helfen!

09.04.2020

Für Interessierte: Ein bisschen Hintergrund zu geheimen Botschaften...

Die Wissenschaft, die sich mit dem Verschlüsseln und Entschlüsseln geheimer Botschaften befasst, ist die **Kryptographie**. Um seine Botschaft zu verschlüsseln, erstellt der Osterhase eine Permutation. Es werden die Zeichen der Nachricht nach einer festen Vorgabe in eine andere Reihenfolge gebracht.

Jede Permutation lässt sich als eine Hintereinanderausführung von Vertauschungen einzelner Buchstaben darstellen. Das Vertauschen zweier Zeichen in einer Menge mit fester Reihenfolge heißt **Transposition**. Es stellt eines der beiden wichtigsten klassischen kryptographischen Verfahren dar, um Nachrichten zu verschlüsseln. Das andere ist die **Substitution**. Hier werden die Zeichen der Nachricht nach einem festen Schema mit anderen Zeichen ersetzt. Der folgende Begriff wurde mit der Caesar-Verschlüsselung verschlüsselt:

Y U Z F A E F Q D C G U L

Jetzt darfst du noch mal knobeln: Recherchiere wie die Caesar-Verschlüsselung funktioniert. Kannst du den Text zu knacken?

(Hinweis: Die Buchstaben wurden nicht wie bei Julius Caesar nur um drei Positionen verschoben..).

Wichtig bei kryptographischen Verfahren ist, dass sich die Zeichen auch wieder eindeutig entschlüsseln lassen. Wenn z.B. Buchstaben einer Nachricht einfach nur alphabetisch geordnet werden würden, wäre bei "EENRTT" nicht klar, ob das Wort vorher "treten" oder "retten" hieß. Inhaltlich macht das einen wesentlichen Unterschied.

Um diese Eindeutigkeit zu garantieren, werden in der modernen Kryptographie Verschlüsselungen durch **umkehrbare mathematische Funktionen** beschrieben. Eine Funktion gewährleistet nach Definition, dass die Botschaft in einen eindeutigen Geheimtext umgeformt wird. Durch die Umkehrbarkeit wird der Geheimtext auch garantiert wieder in die richtige Botschaft zurückgebracht.

Da Computer alle unsere Daten im Hintergrund in Zahlen umwandeln, lassen sich damit alle unsere Nachrichten verschlüsseln. Bei verschlüsselten Verbindungen im Alltag, also zum Beispiel bei Online Shopping, Banking, WhatsApp und vielem mehr, werden dann Verfahren angewandt, die aus einer Kombination aus Transpositionen, Substitutionen und weiteren mathematischen Verfahren bestehen.