Die CÄSAR-Verschlüsselung

Think – Pair – Share:

Think:

1. *Entschlüssle den folgenden Geheimtext (Info: der Klartext ist in deutscher Sprache):*

   NMAB OMUICMZB QV LMZ MZLMV ABMPB LQM NWZU ICA TMPU OMJZIVVB

   PMCBM UCAA LQM OTWKSM EMZLMV NZQAKP OMAMTTMV AMQL HCZ PIVL

   DWV LMZ ABQZVM PMQAA ZQVVMV UCAA LMZ AKPEMQAA AWTT LIA EMZS LMV UMQABMZ TWJMV LWKP LMZ AMOMV SWUUB DWV WJMV

   Solltest du damit Schwierigkeiten haben: Schau dir den Tipp auf dem Pult an.

2. *„Wie hängen Geheim- und Klaralphabet zusammen?“ Schreibe unter die jeweiligen Buchstaben des Klaralphabets (obere Zeile) die zugehörigen des Geheimalphabets in die untere Zeile:*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Formuliere eine Regel, wie man von einem Klar- zu einem Geheimbuchstaben kommt → ***Schlüssel e für Verschlüsselung*** *(encryption):*

Man geht im Alphabet 8 Buchstaben nach rechts (oder 18 Buchstaben nach links)

Pair:

3. *Vergleicht eure Ergebnisse.*

Als „mathematische Schlüssel“ bieten sich an: -8 oder +18. Allerdings kann man dabei über den Bereich 0 bis 25 hinauskommen. Der Schlüssel (Klarbuchstabe - 8) mod26 (bzw. Klarbuchstabe +18) mod26) löst das Problem.

….

Die kürzeste Möglichkeit, einen Schlüssel e der CÄSAR-Verschlüsselung anzugeben, ist *Addition (bzw. Subtraktion) von e.* *Wenn man über die Zahl 25 hinaus (bzw. unter die Zahl 0) gelangt, muss man die Formel erweitern:*

(Klarbuchstabe ± e) mod 26