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

*Formuliere eine Regel, wie man von einem Klar- zu einem Geheimbuchstaben kommt, d.h. formuliere einen **Schlüssel e für Verschlüsselung** (encryption):*

_____

Pair:

3. *Vergleicht eure Ergebnisse. Stellt euch vor, ihr müsst die Schlüssel übermitteln. Je kürzer das möglich ist, umso besser. Tipp: Dazu kann kann man jedem Buchstaben eine Zahl zuordnen. Formuliert die „Schlüssel“, wie man mathematisch von einem Klarbuchstaben zu einem Geheimbuchstaben kommt, so kompakt wie möglich.*

4. *Verschlüsselt einen neuen (kurzen!) Text eurer Wahl mit einem neuen Schlüssel. Gebt diesen Geheimtext mit dem kompakt formulierten Schlüssel an eine andere Gruppe weiter, die die Nachricht entschlüsseln soll.*

Share:

5. *Tauscht euch mit anderen Gruppen aus:*
   - ➢ *Habt ihr dieselbe Übermittlungsmöglichkeit gefunden?*
   - ➢ *Falls NEIN: Erklärt euch eure Möglichkeiten gegenseitig. Leisten sie das selbe?*
   - ➢ *Welche ist kompakter und damit besser (weil schwerer abzufangen)?*

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