

Cäsar und die modulare Arithmetik - Lösung

1. Ergänze die Cäsar-Tabelle. Verschiebe dabei das Alphabet um 9 Stellen nach LINKS!

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

2. Verschlüssele nun: G U T. : _____ **P D C** _____

3. Statt mit Buchstaben arbeiten wir nun mit Zahlen. Ordne dazu jedem Buchstaben zunächst eine Zahl zu, beginnend bei 0.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Verrechnung Zahl des Klartextbuchstaben mit dem Schlüssel:

Zur Zahl des Klartextbuchstaben muss der Schlüssel (9) addiert werden:

4. Verschlüssele nun mit dem folgenden Verfahren:

Schreibe den Buchstaben als Zahl → addiere den Schlüssel → schreibe als Buchstaben

G → **6** → **15** → **P**

U → **20** → **29** → **? (muss D ergeben)**

T → **19** → **28** → **? (muss C ergeben)**

5. Beschreibe, welches Problem bei R auftritt. **Die Zahl ist größer als 25**

6. Lösung mit Hilfe der modulo-Rechnung: **Nach dem Durchlaufen des Alphabets fangen die Zahlen wieder bei 0 an. Also: rechne (Klartextbuchstabe + 9) mod 26**

7. Stelle einen einzigen Term auf, mit dem sich die Nummer des Geheim-Buchstaben aus der Nummer des Klartext-Buchstaben (auch für die Problemfälle) berechnen lässt.

_(Zahl + 9) mod 26) (bzw. (Zahl - 17) mod 26) _____

8. Term für das Entschlüsseln: **(Zahl - 9) mod 26** _____

9. Entschlüsselung auch als ADDITION (wenn du sie in 8. schon als Addition geschrieben hast: Wie lautet die gleichwertige Subtraktion dazu?):

(Zahl + 17) mod 26 (bzw. (Zahl - 9) mod 26) _____

10. SUPER mit dem Schlüssel 15 → **HDETG**