Cäsar und die modulare Arithmetik - Lösung

1.

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. *G U T verschlüsselt mit s=9:* _____*P D C*_____

3.

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

4. *Verschlüssle nun mit dem folgenden Verfahren:*
Schreibe den Buchstaben als Zahl → addiere den Schlüssel → schreibe als Buchstaben

G	→ 6	→	6 + 9 = 15 → 15
U	→ 20	→	20 + 9 = 29 → ??? D (3)
T	→ 19	→	19 + 9 = 28 → ??? C (2)

5. Die Zahlen werden größer als 25.

6. Rechne mod 26

7. (Klartextbuchstabe + Schlüssel) mod 26 = Kryptobuchstabe

8. (Kryptobuchstabe - Schlüssel) mod 26 = Klartextbuchstabe

(16-9)mod26 = 7 (4-9)mod26 = -5 mod26 = 21 (3-9)mod26 = -6 mod26 = 20

Hinweis: Die Java-Operation % berechnet für negative Zahlen nicht das Gleiche wie mod erwarten lassen würde.

9. *S*timmt weil: (K-S)mod26 = (K+26-S)mod26

10. Im Vigenere Verfahren, im One-Time-Pad, in der Skytale-Verschlüsselung und vielen anderen.