Agenda zu Verschlüsselung

- Definition
- Verschlüsselungsverfahren
  - Cäsar
  - One Time Pad
  - Vigenere

Definition

Verschlüsselung und Kryptographie

Was ist Verschlüsselung und welches Ziel hat sie?

- Umwandlung von **"Klartext"** in **"Geheimtext"**. Dies geschieht mit Hilfe eines **geheimen Schlüssels**.
- **Ziel: Informationen für Unbefugte unverständlich machen!**

Was bedeutet Kryptographie?

- **Wissenschaft** des **Verschlüsselns**.
  ►Nicht zu verwechseln mit der Verschlüsselung selbst.

Was sind Ziele der Kryptographie?

- **Vertraulichkeit:** Zugriff nur für bestimmte Personen
- **Integrität:** Schutz vor Änderungen
- **Authentizität:** Identifikation vom Absender
  (z.B. durch „Signaturen“ oder „Zertifikate“)
- **Verbindlichkeit:** Absender ist verantwortlich für Inhalt.
  (Als Konsequenz der Authentizität)

Cäsar

Buchstaben verschieben

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Cäsar-Verschlüsselung

Klartext:	H	A	L	L	O
Schlüssel:	1				
Geheimtext:	I	B	M	M	P

Schlüssel ist Zahl

Jeder **Buchstabe** vom Klartext wird um eine bestimmte Anzahl von Stellen im Alphabet **verschoben**, wodurch Geheimtext entsteht.

Fazit:

Sehr **unsicher** und nur zu **Lernzwecken** verwendet!

Normale Cäsar-Verschlüsselung

Umgekehrte Cäsar-Verschlüsselung

Übung

Verschlüsseln Sie folgende Texte mittels Cäsar-Verschlüsselung.

Klartext	Schlüssel	Geheimtext
HALLO	1	IBMMP
HALLO	2	JCNNQ
WELT	3	ZHOW
WELT	1	XFMU

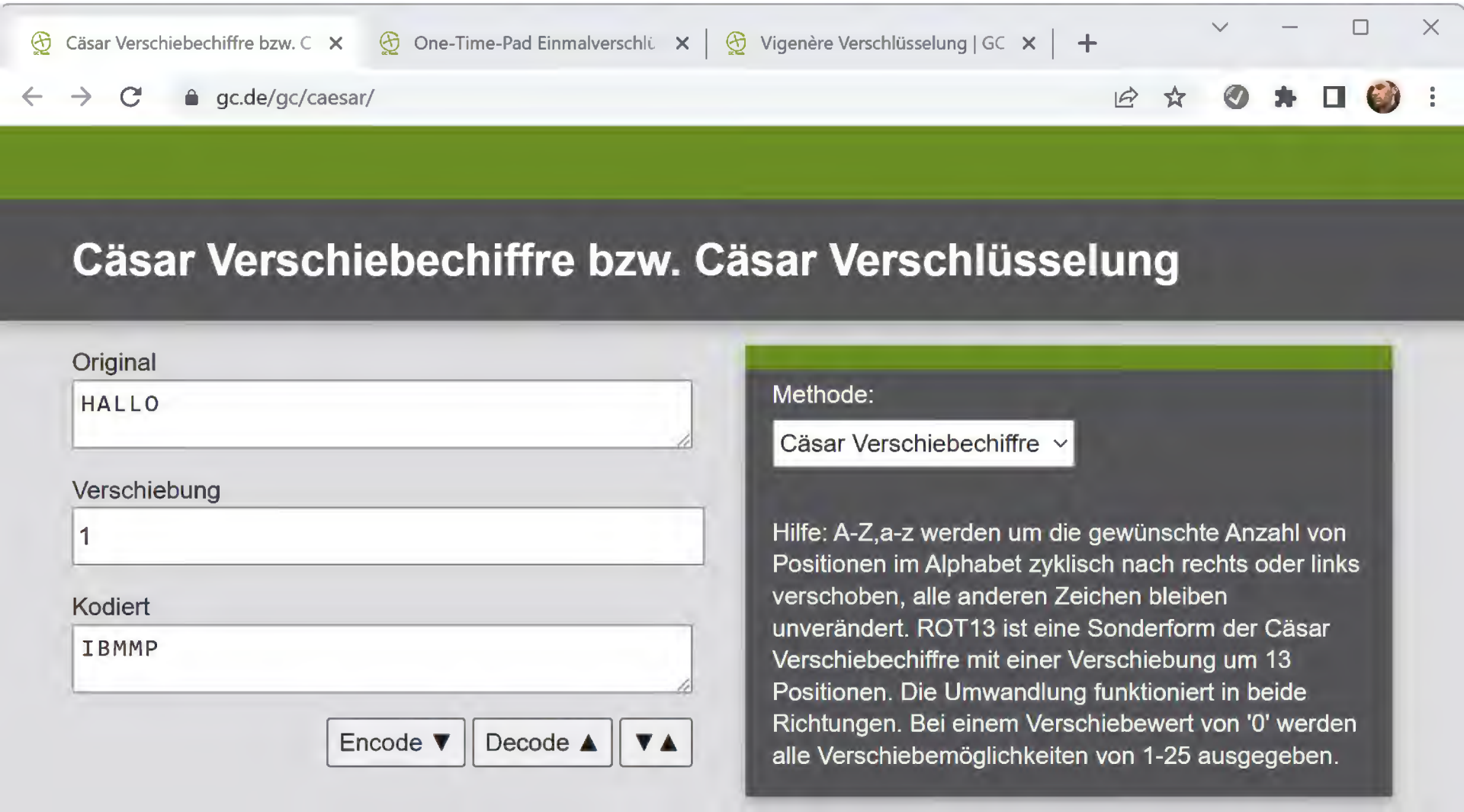
Übung

Entschlüsseln Sie folgende Texte mittels Cäsar-Verschlüsselung.

Geheimtext	Schlüssel	Klartext
UFYU	1	TEXT
OCWU	2	MAUS
FRGH	3	CODE
EBUFO	1	DATEN

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Webseite: https://gc.de/gc/caesar



One-Time-Pad

Buchstaben addieren

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

OTP-Verschlüsselung

Klartext:	H	A	L	L	O
Schlüssel:	A	B	A	B	B
Geheimtext:	H	B	L	M	P

Schlüssel ist Text
(gleichlang wie Klartext)

Jeder **Buchstabe** vom Klartext wird mit dem entsprechenden Buchstaben vom Schlüssel **verknüpft**, wodurch Geheimtext entsteht. Zur Verknüpfung wird Addition verwendet (Erklärung folgt).

Fazit:

Sehr **sicher, wenn der Schlüssel wechselt (One-Time)** und aus **Zufallsbuchstaben** besteht.

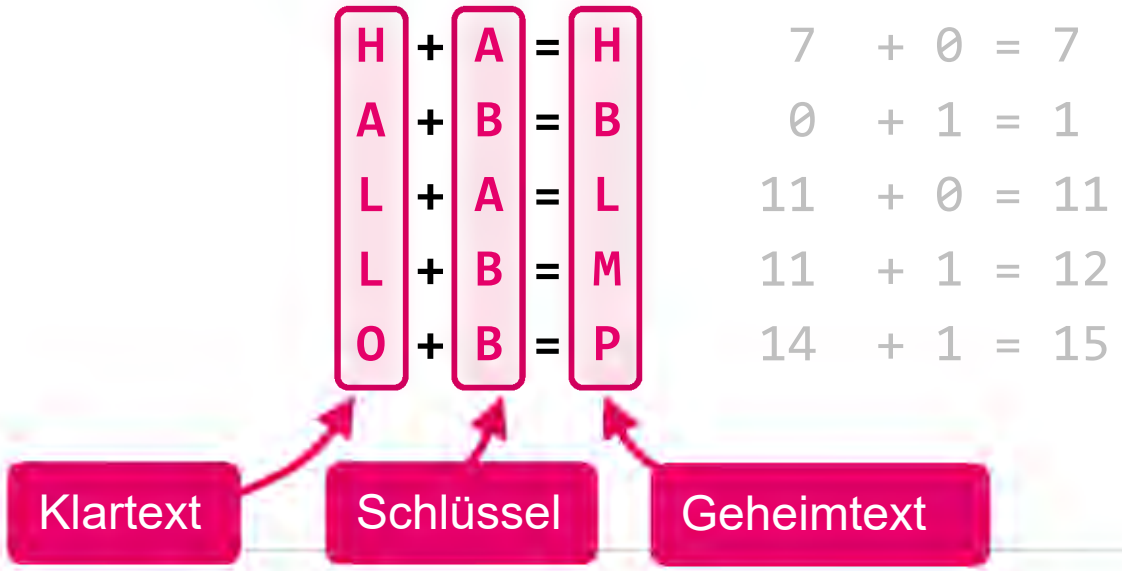
Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Erklärung (Variante A=0)

1. Tabelle mit Buchstaben und Zahlen notieren

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

2. Addition von Buchstaben (Klartext + Schlüssel)



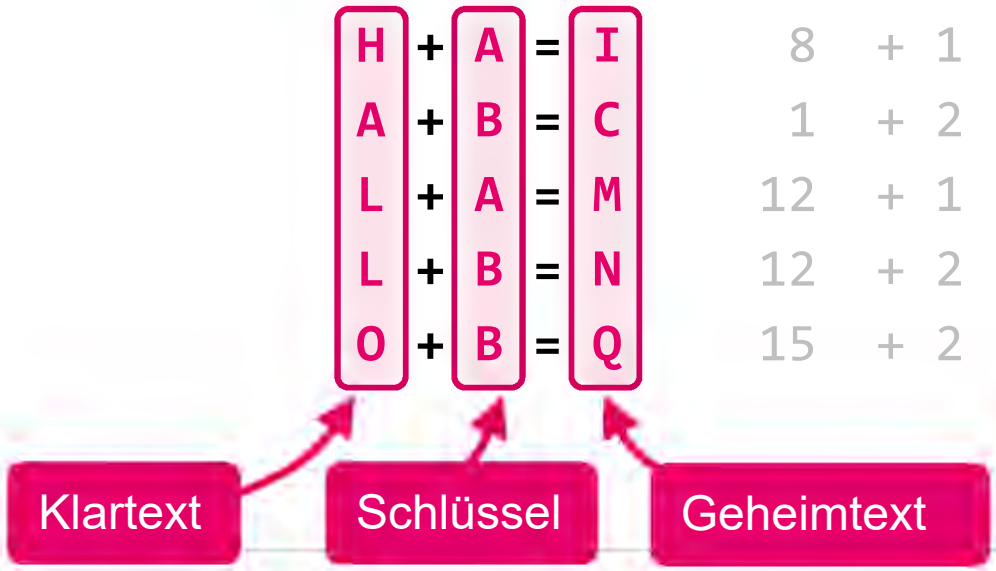
Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Erklärung (Variante A=1)

1. Tabelle mit Buchstaben und Zahlen notieren

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
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	26

2. Addition von Buchstaben (Klartext + Schlüssel)



Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Übung

Verschlüsseln Sie folgende Texte mittels OTP-Verschlüsselung (Variante A=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
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	26
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Klartext	Schlüssel	Geheimtext	Rechnung
HALLO	GEHEI	OFTQX	8+7 |1+5 |12+8 |12+5|15+9
WELT	GEHE	DJTY	23+7|5+5 |12+8 |20+5
TEXT	DING	XNLA	20+4|5+9 |24+14|20+7
CODEN	DINGS	GXRLG	3+4 |15+9|4+14 |5+7|14+19

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Übung

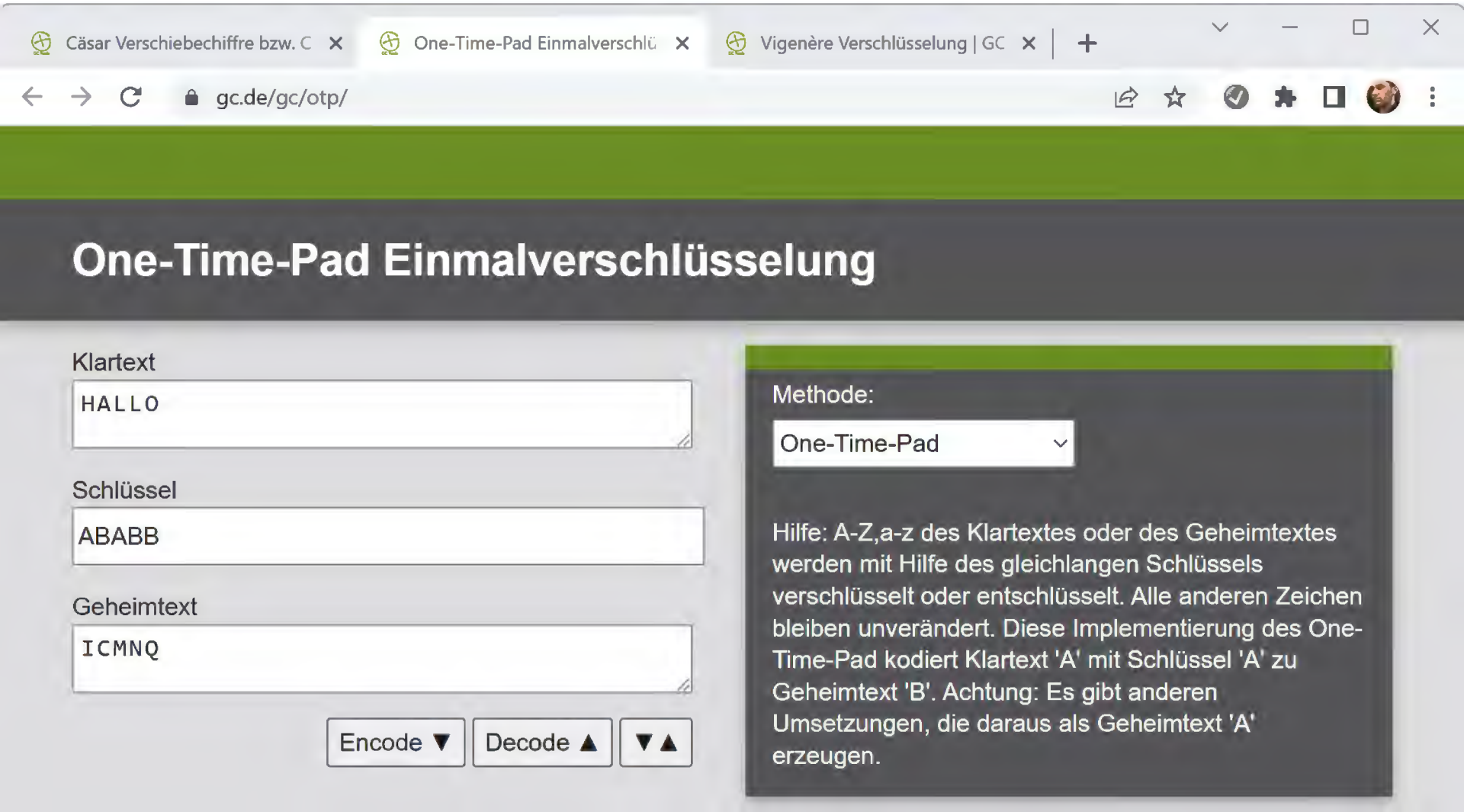
Entschlüsseln Sie folgende Texte mittels OTP-Verschlüsselung (Variante A=1).

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
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	26
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	9	8	8	7	6	5	4	3	2	1	0

Geheimtext	Schlüssel	Klartext	Rechnung
AMOS	ALTE	ZAUN	1-1 |13-12|15-20|19-5
NMOX	ALTE	MAUS	14-1 |13-12|15-20|24-5
ZTPY	WELT	CODE	26-23|20-5 |16-12|25-20
AFFYS	WELTE	DATEN	1-23 |6-5 |6-12 |25-20|19-5

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Webseite: https://gc.de/gc/otp



Vigenère

Cäsar

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Vigenère-Verschlüsselung

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

Schlüssel: H A L L O

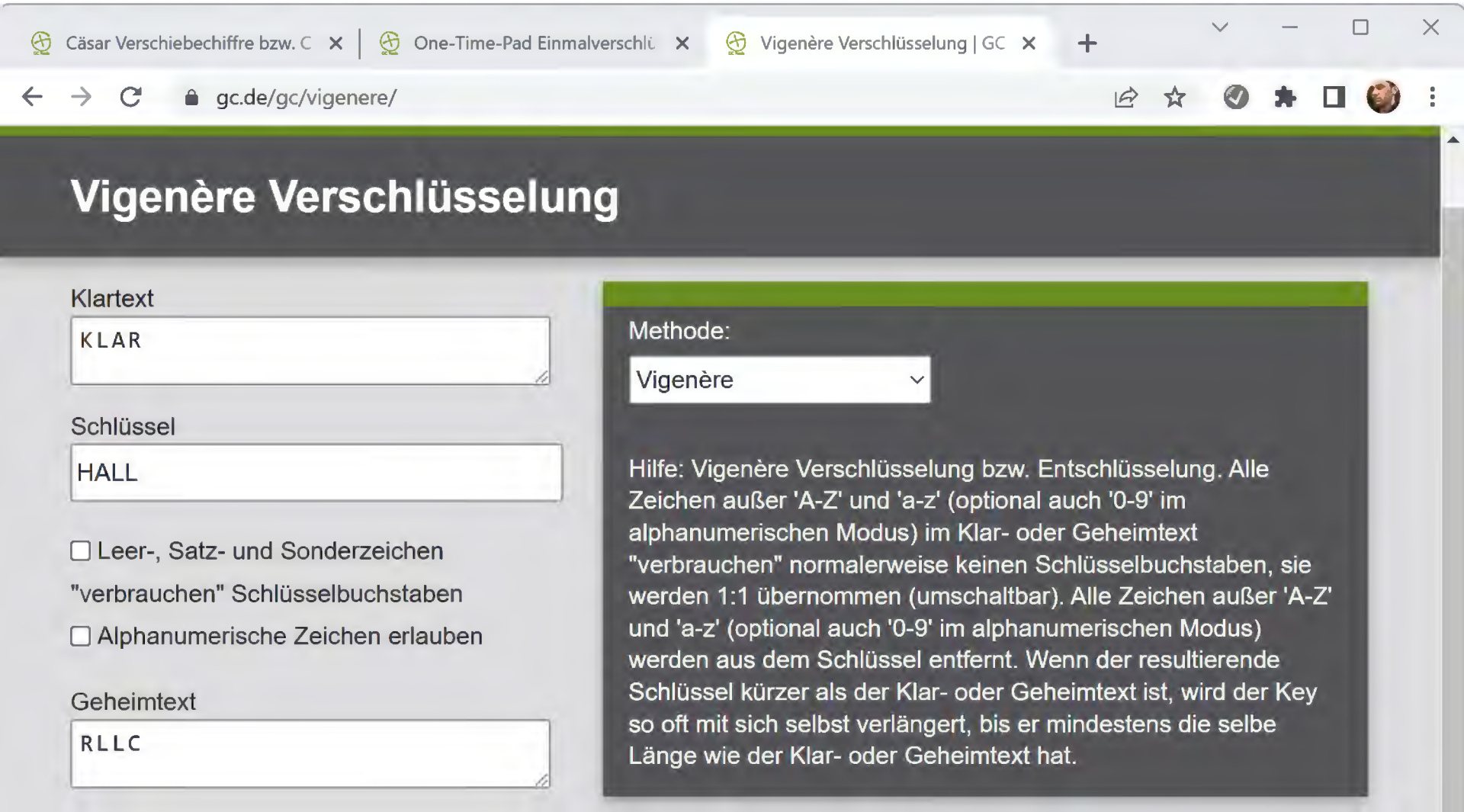
Klartext: K L A R
H A L L

Geheimtext: R L L C

Entschlüsseln: R L L C
H A L L
K L A R

Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Webseite: https://gc.de/gc/vigenere



Realschule Monte Sole
Schule mit Herz und Profil: betreuen und fördern.

Erklärung

1. Tabelle mit Buchstabenquadrat notieren

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