Caesar

Substitution (monoalphabetisch)

Die Buchstaben bleiben **wo** sie sind, aber nicht **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

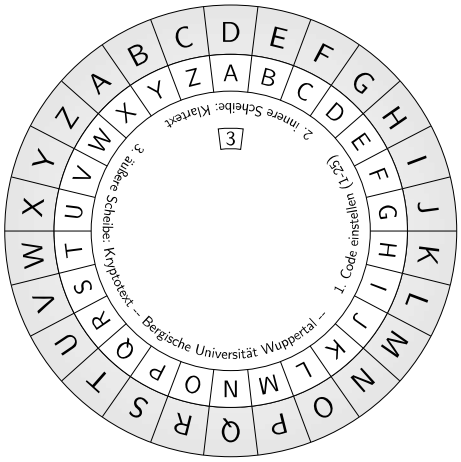
Der römische Feldherr Julius Caesar (100 bis 44 v. Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Diese Anzahl der Stellen heißt **Caesar-Schlüssel**.

Beispiel Beim Schlüssel **3** nahm Caesar immer den Buchstaben, der im Alphabet drei Stellen weiter rechts steht.
Dazu schrieb er das Alphabet zweimal untereinander. Das untere Alphabet schrieb er allerdings um drei Stellen verschoben.

	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
wird ersetzt durch	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

Caesar ersetzte also in seinem Text jedes **A** durch ein **D**, jedes **B** durch ein **E** usw. Beachte, dass **X** durch **A** ersetzt wird, also das Alphabet nach dem Z einfach mit A weitergeschrieben wird.

Damit nicht jedesmal die beiden gegeneinander verschobenen Alphabete aufgeschrieben werden müssen, kann auch eine sogenannte Chiffrierscheibe benutzt werden. In der Abbildung ist wie im Beispiel der Schlüssel 3 eingestellt.
Mit der Scheibe kannst du nun sowohl Texte verschlüsseln als auch entschlüsseln. Möchtest du verschlüsseln, dann suchst du den Buchstaben auf der inneren Scheibe und schreibst den entsprechenden Buchstaben auf der äußeren Scheibe auf. Entschlüsseln geht entsprechend umgekehrt: Hier suchst du den Buchstaben außen und schreibst den entsprechenden Buchstaben auf der inneren Scheibe auf.



v3 29. Mai 2012

Caesar

Substitution (monoalphabetisch)

Die »normale« Caesar-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird.
Diese Verschlüsselung funktioniert so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort.
- Dieses Wort schreibst du unter ein normales Alphabet. Buchstaben, die doppelt vorkommen, lässt du dabei weg.
- Anschließend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt. Kein Buchstabe darf doppelt vorkommen.

Beispiel Schlüsselwort: GEHEIMSCHRIFT. Dieses Schlüsselwort wird unter das Alphabet geschrieben, doppelte Buchstaben werden dabei weggelassen.

	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
wird ersetzt durch	G	E	H	I	M	S	C	R	F	T																

Nun wird mit den restlichen Buchstaben aufgefüllt.

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

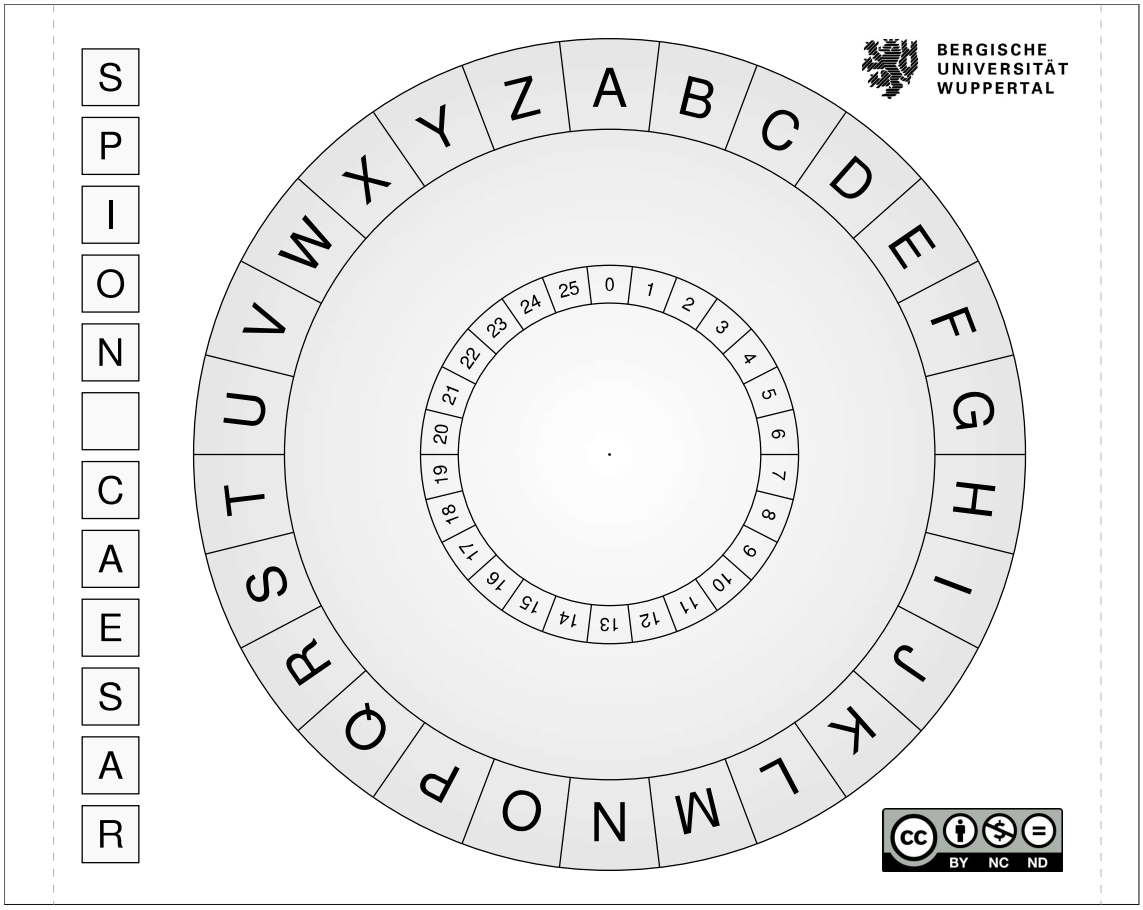
Mit dieser Tabelle wird dann ver- und entschlüsselt.

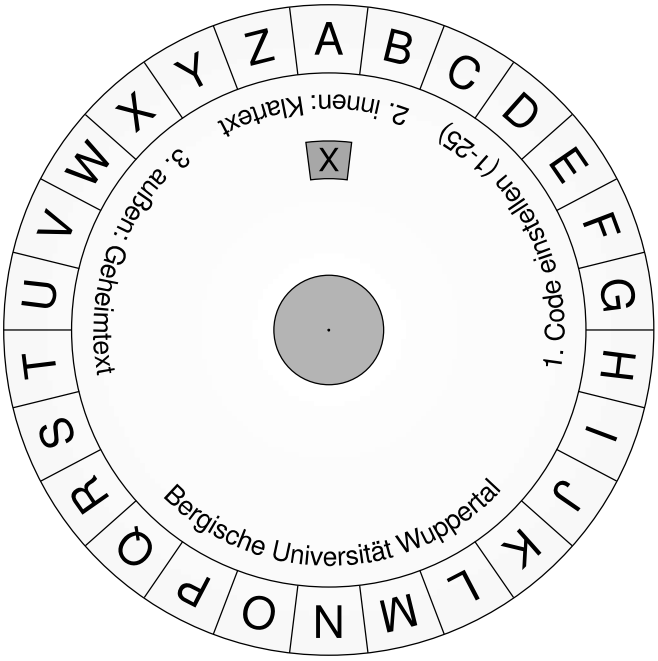
v3 29. Mai 2012

BERGISCHE UNIVERSITÄT WUPPERTAL

Caesar

Substitution (monoalphabetisch)





Caesar

Substitution (monoalphabetisch)

Bergische Universität Wuppertal - SpionCamp - Caesar

S P I O N _ C A E S A R

Verschlüsseln

Stelle den Caesarcode (1-25) mit der inneren Scheibe ein. Nimm den Klartext und schaue jeden Buchstaben auf der inneren Scheibe nach. Auf der äußeren Scheibe steht der entsprechende Geheimtext.

Entschlüsseln

Stelle den Caesarcode (1-25) mit der inneren Scheibe ein. Nimm den Geheimtext und schaue jeden Buchstaben auf der äußeren Scheibe nach. Auf der inneren Scheibe steht der entsprechende Klartext.

BERGISCHE UNIVERSITÄT WUPPERTAL

Bergische Universität Wuppertal - SpionCamp - Caesar

S P I O N _ C A E S A R

- Beim Ausdruck darauf achten, dass das Dokument nicht skaliert gedruckt wird (CD-Hüllenbreite: 15cm)
- Durchmesser großes Rad: 11cm, klein: 8,6cm
- Laminieren der kleinen Scheibe empfohlen!
- Kleines Rad ausschneiden und graues Code-Fenster (X) ausschneiden
- Falls eine CD-Hülle verwendet wird: Den inneren Ring aus dem kleinen Rad herausschneiden
- Großes Rad mit dem CD-Hüllen-Rand oder ohne diesen ausschneiden
- Falls keine CD-Hülle verwendet wird: die Scheiben mit einer Musterbeutelklammer  verbinden

Aufgabe 1 Könnt ihr die Nachricht ohne bekannten Schlüssel entschlüsseln?
YHQL YLGL YLFL

Aufgabe 2 Entschlüsselt mit der Chiffrierscheibe die folgenden Nachrichten. Mögliche Schlüssel sind: **2**, **7**, **10**, **13.** Einer ist jeweils der richtige Schlüssel. Das heißt, dass man bei Verschiebung um diese Zahl die Nachricht erhält.

a) **SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU?**

b) **YVRORE PNRFNE, VPU JREQR QN FRVA.**

Aufgabe 3 Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

Aufgabe 4 Verschlüsselt und entschlüsselt gegenseitig den Titel eures Lieblingsbuches mit dem Schlüsselwort **LESERATTE**.

Aufgabe 5 Entschlüssele die folgende Nachricht. Das Schüsselwort ist **SCHATZSUCHE** oder **MEISTERDETEKTIV**.

STG HIKMJU YVTDJ KVAJTG STG CMGXEMAX

Aufgabe 6 Was ist der Vorteil bei dem Schlüsselwort-Caesar-Verfahren?

Aufgabe 7 Fällt dir eine Möglichkeit ein, wie du einen Text entschlüsseln kannst, ohne alle Schlüssel durchzuprobieren? *Tipp:* Nutze dabei eine bestimmte Eigenschaft einer Sprache (z. B. Deutsch) aus.

v2 1. Dezember 2011