Station 2 – Caesar

Hintergrund

Die Caesar-verschlüsselung geht auf den römischen Feldherren Gaius Julius Caesar (100 v. Chr. Bis 44 v. Chr.) zurück.

Ursprünglich hatte Caesar die Ersetzung der Buchstaben durch andere im Gallischen Krieg beschrieben. Er musste eine Botschaft an den belagerten Quintus Cicero schicken, der kurz davor war, sich zu ergeben. Damit die Feinde die Botschaft nicht lesen konnten, schrieb Caesar sie mit griechischen Buchstaben auf und beauftragte einen Boten, sie zu überbringen. Sollte der Bote es nicht bis zum Lager schaffen, sollte er sie an einen Wurfspeer befestigen und sie ins Lager schleudern. Der Speer blieb zwar in der Pallisade des Römerlagers stecken, viel aber einer Wache auf. Die Belagerten schöpften neuen Mut.

Der römische Schriftsteller und Beamte Sueton beschrieb in seinem Werk Kaiserviten, dass Caesar geheime Botschaften aufschrieb, indem er die Buchstaben um drei Stellen im Alphabet verschob. “Um diese zu lesen, tauscht man den vierten Buchstaben, also D für A, aus und ebenso mit den restlichen.” (De Vita Caesarum: Divus Julius LVI)

Auch der römische Kaiser Augustus hat später das Verfahren verwendet, hat die Buchstaben aber nur um eine Position verschoben.

Der italienische Universalgelehrte Leon Battista Alberti vereinfachte das Verfahren im 15. Jahrhundert durch die Erfindung der Chiffrierscheibe. An dieser Station könnt ihr euch eine eigene Chiffrierscheibe bauen.

Quelle: Wikimedia Commons - https://commons.wikimedia.org/wiki/File:CipherDisk2000.jpg

Prinzip

Bei der Caesar-Verschlüsselung handelt es sich um eine einfache Verschlüsselung, bei der die Buchstaben im Alphabet einfach um eine bestimmte Anzahl Buchstaben verschoben werden.

Man kann sich das leichter vorstellen, wenn man das Alphabet des unverschlüsselten Klartextes und das Alphabet des verschlüsselten Geheimtextes übereinanderschreibt. Ohne Verschiebung sieht das so aus:

Klartext:	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
Geheimtext:	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

Jetzt nutzen wir die Verschiebung um drei Buchstaben, so wie sie Caesar angewendet hat. Die Buchstaben, die vorne “runterfallen” würden, fügen wir hinten einfach wieder an.

Klartext:	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
Geheimtext:	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

Will ich einen Text verschlüsseln, gehe ich ihn Buchstabe für Buchstabe durch, sehe nach, durch welchen Buchstaben ich ihn ersetzen muss und schreibe diesen auf. Beim Entschlüsseln gehe ich genauso vor. Ich gehe den geheimen Text Buchstabe für Buchstabe durch und siehe nach, welchem Buchstaben aus dem Klartext er entspricht und schreibe diesen auf.

Die Anzahl der Buchstaben, um die wir das Alphabet verschieben ist der **geheime Schlüssel** der Caesar-Verschlüsselung. Bei dieser Chiffre handelt es sich um eine monoalphabetische Substitution, d.h. dass für die Verschlüsselung eines Textes nur ein Schlüsselalphabet genutzt wird und daher gleiche Buchstaben auch immer mit dem gleichen Buchstaben ausgetauscht werden. Es handelt sich um ein symmetrisches Verschlüselungsverfahren, da zum ver- und entschlüsseln der gleiche Schlüssel genutzt wird. Dieser muss vorher zwischen den Teilnehmer*innen der Kommunikation über einen sicheren Weg ausgetauscht werden.

Die klassische Caesar-Verschlüsselung rotiert da Alphabet, so dass sie auch als ROT3 bezeichnet wird. ROT 3 ist eine Verschiebung um 3 stellen. ROT13 um 13 Stellen. Auf den Vordrucken für die Chiffrierscheiben ist diese Zahl jeweils mit angegeben.

Beispiel

Verschlüsselung

Ich möchte folgenden Text verschlüsseln:

Hallo liebe Besucherinnen und Besucher,

Herzlich Willkommen an der Station zur Caesar-Verchlüsselung.

Als geheimen Schlüssel wähle ich wie Caesar den Wert 3. D.h. ich habe folgende Tabelle zur Verschlüsselung meines Textes.

Klartext:	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
Geheimtext:	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

Somit ergibt sich aus dem H ein K, aus a ein d, aus l ein o und so weiter. Der gesamte verschlüsselte Text lautet dannwie folgt:

Kdoor olheh Ehvxfkhulqqhq xqg Ehvxfkhu,

KhuColfk Zloonrpphq dq ghu Vwdwlrq Cxu Fdhvdu-Yhufkoüvvhoxqj.

Entschlüsselung

Nun möchte ich den Text als Empfänger*in wieder entschlüsseln.

Kdoor olheh Ehvxfkhulqqhq xqg Ehvxfkhu,

KhuColfk Zloonrpphq dq ghu Vwdwlrq Cxu Fdhvdu-Yhufkoüvvhoxqj.

Ich kenne den geheimen Schlüssel 3 und kann mir daher wieder eine Tabelle aufschreiben. Diesmal ist das Alphabet des Geheimtextes oben und dasjenige des Klartextes unten. Die Verschiebung der Buchstaben führe ich diesmal in die andere Richtung durch.

Geheimtext:	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
Klartext:	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

Somit ergibt sich aus dem K ein H, aus dem d ein a, aus dem o ein l und so weiter. Die gesamte entschlüsselte Nachricht lautet dann wieder:

Hallo liebe Besucherinnen und Besucher,

Herzlich Willkommen an der Station zur Caesar-Verchlüsselung.

Angriffe

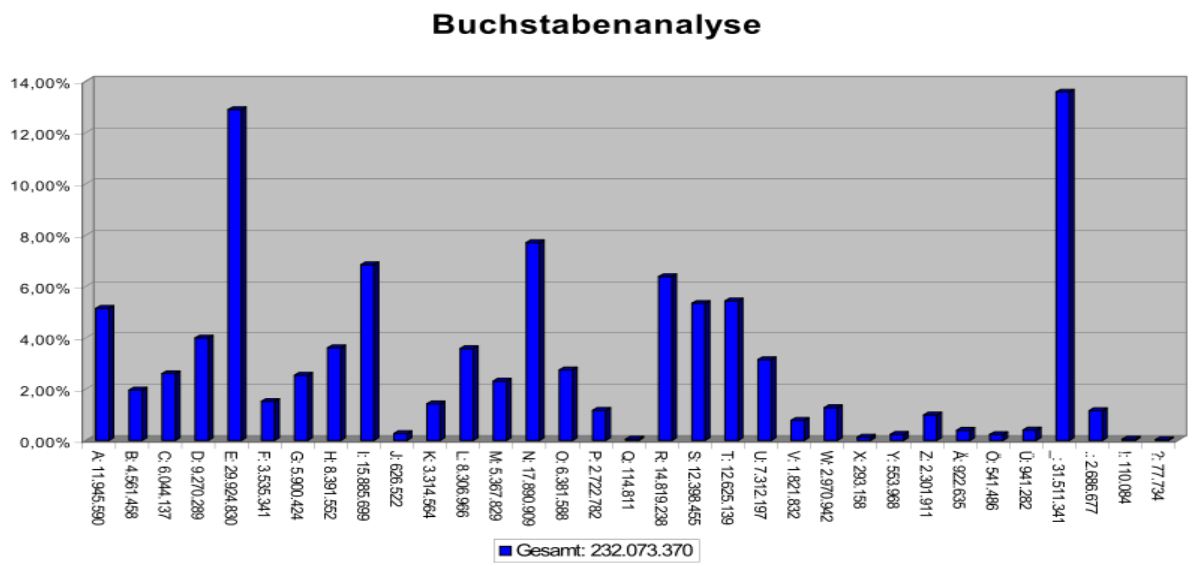
Brute-Force

Die Caesar-Verchlüsselung ist eine relativ schwache Verschlüsselung. Ihr stehen nur 25 Schlüssel zur Verfügung, die sich auch schnell durchprobieren lassen. Bereits bei den ersten paar Buchtaben kann man ja sehen, ob es ein sinnvolles Wort ergeben wird. Das bloße Durchprobieren von möglichen Schlüsseln nennt man auch Brute-Force-Angriff.

Häufigkeitsanalyse

Neben dem simplen Durchprobieren sind monoalphabetische Verschlüsselungen wie Caesar auch anfällig für feinere Angriffe. Der arabische Gelehrte al-Kindī entwickelte im 9. Jahrhundert die Häufigkeitsanalyse als kryptografisches Verfahren. Erst viele Jahre später kam das Verfahren nach

Europa. Die Häufigkeit der Buchstaben ist in einer Sprache nicht gleich verteilt. Im Deutschen kommt das E mit Abstand am häufigsten vor. Das lässt sich für die Analyse ausnutzen.



Quelle: Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Alphabet_haufigkeit.svg

Mit einer Häufigkeitsanalyse lässt sich ermitteln, welche Zeichen in einem verschlüsselten Text am häufigsten vorkommen. Wenn es merkliche Unterschiede zwischen den Zeichen gibt, handelt es sich vermutlich um eine monoalphabetische Verschlüsselung wie Caesar.

Da es sich um einen Text handelt, bei dem gleiche Buchstaben immer mit dem gleichen geheimen Buchstaben ersetzt werden, bleibt die Häufigkeit erhalten. D.h. dass jetzt der geheime Buchstabe, der für das E steht, am häufigsten im Text vorkommt.

Kommt z.B. das X am häufigsten vor, können wir davon ausgehen, dass X ein verschlüsseltes E ist und somit eine Verschiebung um 19 Buchstaben vorliegt.

Hier ein Beispiel:

WBxLxK mxQM LHEE FBM xBGxK TGtERLx wxK aäNyBzDxBMxG wxK UNvALMtuxG xGMLvAEüLLxEM PxKwxG.

Das X kommt 15-mal vor und hat somit eine Häufigkeit von grob 19%. Somit gehen wir davon au, dass X im Klartext E sein muss und können unsere Entschlüsselungstabelle aufstellen.

Geheimtext:	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
Klartext:	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

Somit lautet der Klartext des Beispiels:

Dieser Text soll mit einer Analyse der Häufigkeiten der Buchstaben entschlüsselt werden.

Ausprobieren

Baue dir deine eigene Chiffrierscheibe

Damit dir das Ver- und Entschlüsseln nach Caesar leichter von der Hand geht, haben wir Material für deine eigene Chiffrierscheibe bereitgelegt.

1. Nimm dir einen Bastelbogen “Chiffrierscheibe”, eine Schere und eine Musterbeutelklammer.
2. Schneide mit der Schere vorsichtig die beiden Scheiben von dem Bastelbogen aus.
3. Bohre mit der Schere jeweils ein Loch in die Mitte der beiden Scheiben.
4. Lege die kleinere Scheibe auf die größere.
5. Verbinde beide Scheiben, indem du die Musterbeutelklammer durchsteckst und auf der anderen Seite auseinanderbiegst.

Welche Besonderheit haben ROT13 und ROT26?

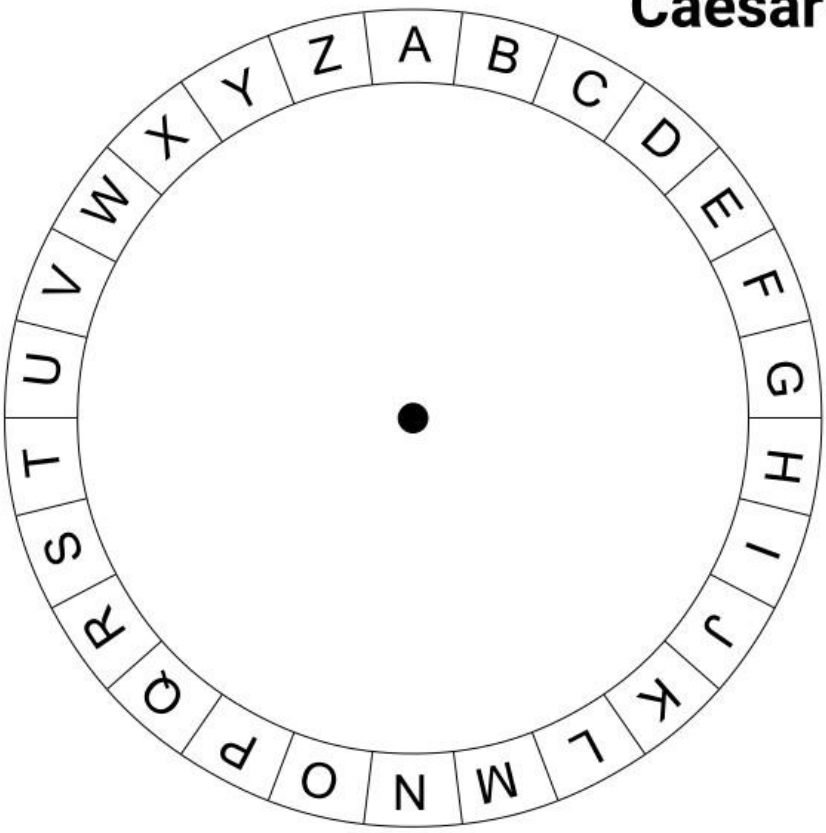
ROT13 hat eine Besonderheit, die sie besonders einfach zum Ver- und Entschlüsseln macht. Kannst du herausfinden, welche das ist?

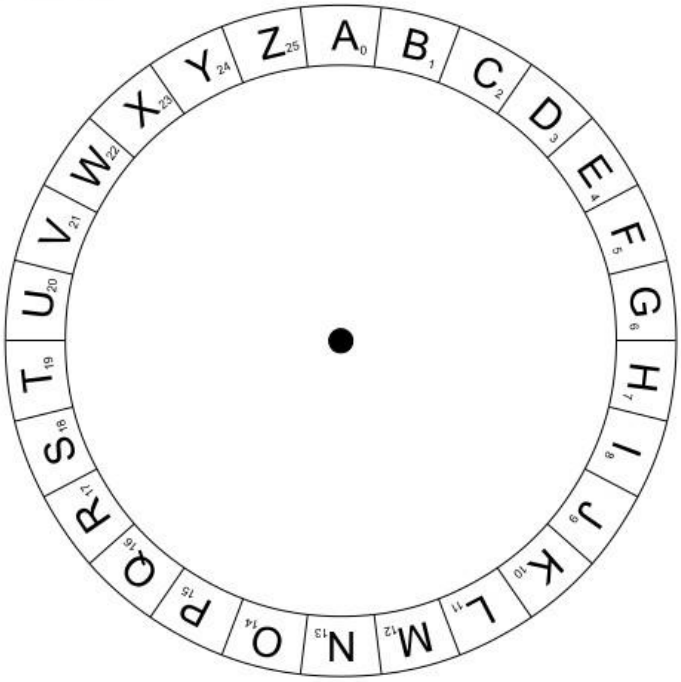
ROT26 wird meistens als Witz von Kryptografen verwendet. Überlege, warum es so unsicher ist?

Entschlüssele den Geheimtext

Wir haben einen kurzen Text mit einer Caesar-Verschlüsselung verschlüsselt. Kannst du den richtigen Schlüssel finden und herausfinden, worum es in dem Text geht?

Caesar-Scheibe





Quelle: https://www.vcp.de/pfadfinden/auf-neuem-pfad/die-caesar-scheibe

Achtung – Erst umdrehen, wenn du deinen Versuch, den Text zu entschlüsseln beendet hast

Geheimtext

PTYP ATKKL (OPFEDNSPC AWFCLW: OTP ATKKLD ZOPC OTP ATKKPY)

TDE PTY GZC OPX MLNVPY HÜCKTR MPWPREPD QWLOPYMCZE LFD

PTYQLNSPX SPQPEPTR LFD OPC TELWTPYTDNSPY VÜNSP. OTP SPFETRP

TYEPCYLETZYLW GPCMCPTEPEP GLCTLYEP XTE EZXLEPYDLFNP FYO

VÄDP LWD MLDTD DELXXE GPCXFEWTNS LFD YPLAPW. 2017 HFCOP OTP

YPLAZWTELYTDNSP VFYDE OPD ATKKLMÄNVPCD (LCE ZQ YPLAZWTELY

‘ATKKLTFZWZ’) GZY OPC FYPDNZ TY OTP CPACÄDPYELETGP WTDEP OPD

TXXLEPCTPWWPY VFWEFCPCMPD OPC XPYDNSSPTE LFQRPYZXXPY.

Achtung – Erst umdrehen, wenn du deinen Versuch, den Text zu entschlüsseln beendet hast

Klartext

Eine Pizza (deutscher Plural: die Pizzas oder die Pizzen) ist ein vor dem Backen würzig belegtes Fladenbrot aus einfachem Hefeteig aus der italienischen Küche. Die heutige international verbreitete Variante mit Tomatensauce und Käse als Basis stammt vermutlich aus Neapel. 2017 wurde die neapolitanische Kunst des Pizzabäckers (Art of Neapolitan ‘Pizzaiuolo’) von der UNESCO in die repräsentative Liste des immateriellen Kulturerbes der Menschheit aufgenommen.

Quelle: https://de.wikipedia.org/wiki/Pizza