Themen

Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung stammt aus dem 16. Jahrhundert und ist nach dem französischen Diplomaten Blaise de Vigenère (1523 – 1596) benannt. Im Gegensatz zur Caesar-Verschlüsselung, bei der die Buchstaben des Klartextes durch Buchstaben eines einzigen Alphabets ersetzt werden, arbeitet man dabei mit 26 Alphabeten. Das Verfahren gehört daher zu den polyalphabetischen Substitutionsverfahren (von lateinisch substituere = „ersetzen“).

Die 26 Alphabete werden – jeweils um eine Stelle verschoben – im Vigenère-Quadrat angeordnet. Welches Alphabet für das Verschlüsseln eines Buchstabens verwendet wird, legt der Schlüssel fest, den Sender und Empfänger der Botschaft kennen müssen.

Beim Verschlüsseln wird das Schlüsselwort (STORCH) über dem Klartext notiert. Der Schlüsselbuchstabe **S** wird in der linken Spalte gesucht. Der Klartextbuchstabe **I** wird in der Zeile oben gesucht. Der Geheimtextbuchstabe A findet sich am Kreuzungspunkt der Spalte **I** mit der Zeile **S**.

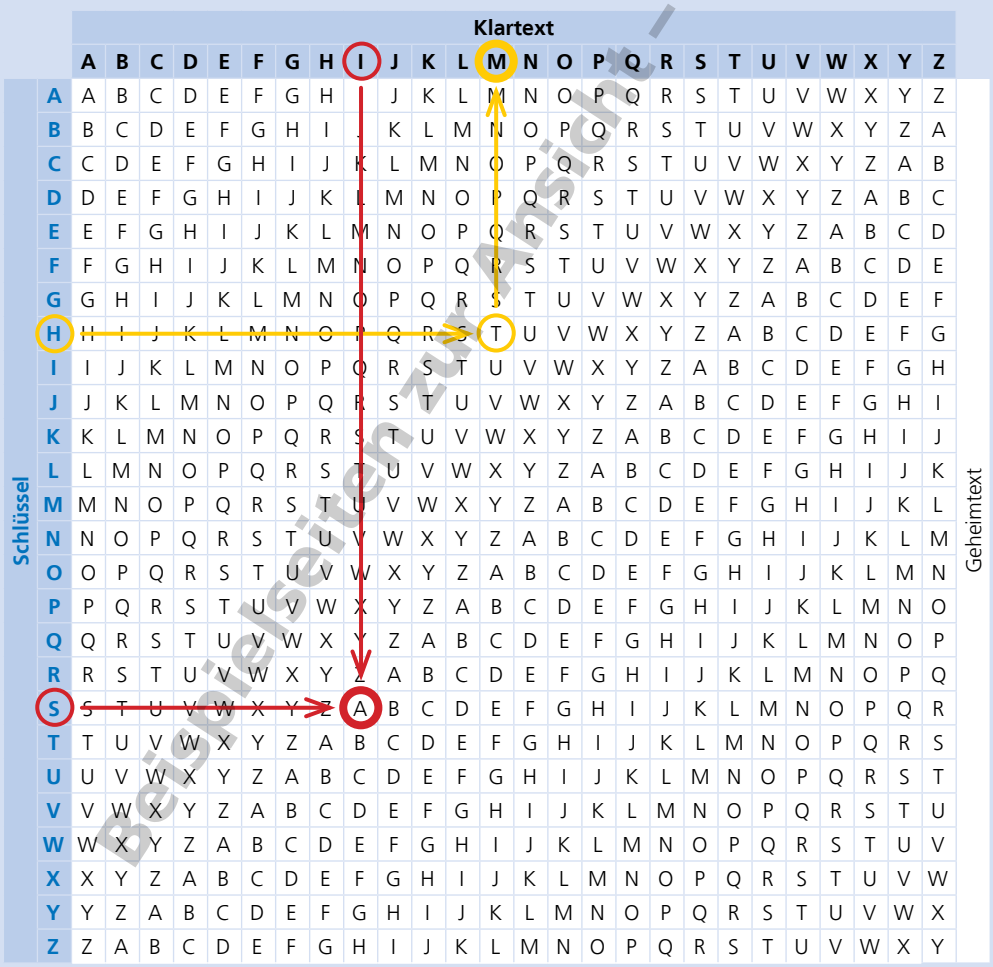
Schlüssel	**S**	**T**	**O**	**R**	**C**	**H**	**S**	**T**	**O**	**R**
Klartext	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**
Geheimtext	A	G	T	F	T	T	S	M	W	B

Beim Entschlüsseln wird der Schlüsselbuchstabe **H** in der linken Spalte gesucht. In der **H**-Zeile sucht man nach dem Geheimtext-Buchstaben T. In der betreffenden Spalte findet sich oben der Klartextbuchstabe **M**.

Schlüssel	**S**	**T**	**O**	**R**	**C**	**H**	**S**	**T**	**O**	**R**
Geheimtext	A	G	T	F	T	T	S	M	W	B
Klartext	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**

Die Vigenère-Verschlüsselung ist deutlich sicherer als die Caesar-Verschlüsselung. Durch das Verschlüsseln gleicher Buchstaben mit unterschiedlichen Schlüsselbuchstaben kann sie nicht durch eine Häufigkeitsanalyse geknackt werden. Für einen Brute-Force-Angriff ist die Anzahl möglicher Schlüssel zu groß.

Dennoch gelang es dem englischen Wissenschaftler Charles Babbage (1791 – 1871) im Jahr 1854 mit dem Vigenère-Verfahren verschlüsselte Texte zu entziffern.



Vigenère-Verschlüsselung

Aufgabe 1
Verschlüssele diese Orte mit dem Schlüsselwort ROM.

MAILAND
BOLOGNA
TURIN
PALERMO
NEAPEL
VERONA

Schlüssel	R	O	M	R	O	M	R
Klartext	**M**	**A**	**I**	**L**	**A**	**N**	**D**
Geheimtext	D	O	U	C	O	Z	U

Schlüssel	R	O	M	R	O	M	R
Klartext	**B**	**O**	**L**	**O**	**G**	**N**	**A**
Geheimtext	S	C	X	F	U	Z	R

Schlüssel	R	O	M	R	O
Klartext	**T**	**U**	**R**	**I**	**N**
Geheimtext	K	I	D	Z	B

Schlüssel	R	O	M	R	O	M	R
Klartext	**P**	**A**	**L**	**E**	**R**	**M**	**O**
Geheimtext	G	O	X	V	F	Y	F

Schlüssel	R	O	M	R	O	M
Klartext	**N**	**E**	**A**	**P**	**E**	**L**
Geheimtext	E	S	M	G	S	X

Schlüssel	R	O	M	R	O	M
Klartext	**V**	**E**	**R**	**O**	**N**	**A**
Geheimtext	M	S	D	F	B	M

MAILAND — DOUCOZU
BOLOGNA — SCXFUZR
TURIN — KIDZB
PALERMO — GOXVFYF
NEAPEL — ESMGSX
VERONA — MSDFBM

Aufgabe 2
Welche Alpenberge sind hier verschlüsselt? (Schlüsselwort: GIPFEL)

FCVXTTZHT
SIIYICNWGS
CIIEQLTV
PCCLJCGC
CQAIWAOBOJ
TMQJPSUZC

Schlüssel	G	I	P	F	E	L	G	I	P
Geheimtext	F	C	V	X	T	T	Z	H	T
Klartext	**Z**	**U**	**G**	**S**	**P**	**I**	**T**	**Z**	**E**

Schlüssel	G	I	P	F	E	L	G	I	P	F
Geheimtext	S	I	I	Y	I	C	N	W	G	S
Klartext	**M**	**A**	**T**	**T**	**E**	**R**	**H**	**O**	**R**	**N**

Schlüssel	G	I	P	F	E	L	G	I
Geheimtext	C	I	I	E	Q	L	T	V
Klartext	**W**	**A**	**T**	**Z**	**M**	**A**	**N**	**N**

Schlüssel	G	I	P	F	E	L	G	I
Geheimtext	P	C	C	L	J	C	G	C
Klartext	**J**	**U**	**N**	**G**	**F**	**R**	**A**	**U**

Schlüssel	G	I	P	F	E	L	G	I	P	F
Geheimtext	C	Q	A	I	W	A	O	B	O	J
Klartext	**W**	**I**	**L**	**D**	**S**	**P**	**I**	**T**	**Z**	**E**

Schlüssel	G	I	P	F	E	L	G	I	P
Geheimtext	T	M	Q	J	P	S	U	Z	C
Klartext	**N**	**E**	**B**	**E**	**L**	**H**	**O**	**R**	**N**

FCVXTTZHT — ZUGSPITZE
SIIYICNWGS — MATTERHORN
CIIEQLTV — WATZMANN
PCCLJCGC — JUNGFRAU
CQAIWAOBOJ — WILDSPITZE
TMQJPSUZC — NEBELHORN

Vigenère-Verschlüsselung

Aufgabe 3

Verschlüssele dieses Zitat, das dem Schriftsteller Mark Twain (1835 – 1910) zugeschrieben wird:
„Das Geheimnis des Vorankommens ist das Anfangen."

Verwende das Schlüsselwort GEHEIM.

DASGE HEIMN ISDES VORAN KOMME NSIST DASAN FANGE N

JEZKM TKMTR QEJIZ ZWDGR RSUYK RZMAF JEZ EV RGRNI V

Aufgabe 4

Entschlüssele die Aussage von Napoléon Bonaparte (1769 – 1821) über das Wetter in Deutschland.

Verwende das Schlüsselwort FRANKREICH.

IZEQO LXAEO JEHNL VRAGJ MJMBX RXMYP SKEEE EHAGJ MJMBX RXMML NEEAC FQUGY

DIEDE UTSCH ENHAB ENSEC HSMON ATEWI NTERU
NDSEC HSMON ATEKE INENS OMMER

„Die Deutschen haben sechs Monate Winter und sechs Monate keinen Sommer."

Schlüssel	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	

Ende-zu-Ende-Verschlüsselung

Mehr als zwei Stunden täglich verbringen Jugendliche und junge Erwachsene mit der Nutzung von Chat- oder Messengerdiensten. Das ergaben Studien zur Mediennutzung von Jugendlichen in Deutschland, die in den „Grunddaten Jugend und Medien 2020“ zusammengefasst sind. [1)]

Selbstverständlich möchte niemand, dass die mit Freundinnen und Freunden ausgetauschten Nachrichten von Dritten mitgelesen werden. Deshalb haben die Anbieter von E-Mail-, Chat- und Messengerdiensten Verfahren zu Verschlüsselung aller übertragenen Daten etabliert.

Problem der Schlüsselverteilung

Bis in die 1970er Jahre hinein kannte man nur symmetrische Verschlüsselungsverfahren, bei denen Sender und Empfänger einer Nachricht über denselben Schlüssel verfügen müssen.

Das führt im Smartphone-Zeitalter zu der Schwierigkeit, dass für viele geheim kommunizierende Personen auch viele unterschiedliche Schlüssel benötigt werden. Die Anzahl lässt sich aus der Anzahl der Messengerdienst-Nutzer errechnen:

$$\text{Anzahl Schlüssel} = \frac{\text{Nutzer} \times (\text{Nutzer} - 1)}{2}$$

Wollten alle zwei Milliarden WhatsApp-Nutzer miteinander verschlüsselte Nachrichten austauschen, wären dafür zwei Trillionen Schlüssel nötig.

Asymmetrische Verschlüsselung

Das so genannte Schlüsselverteilungsproblem wurde erst 1977 gelöst, als Ronald L. Rivest, Adi Shamir und Leonard M. Adleman am Massachusetts Institute of Technology das nach ihnen benannte RSA-Verfahren entwickelten.

Bei diesem ersten asymmetrischen Verschlüsselungsverfahren verfügt jeder Nutzer über ein eigenes Schlüsselpaar: einen öffentlichen und einen privaten Schlüssel.

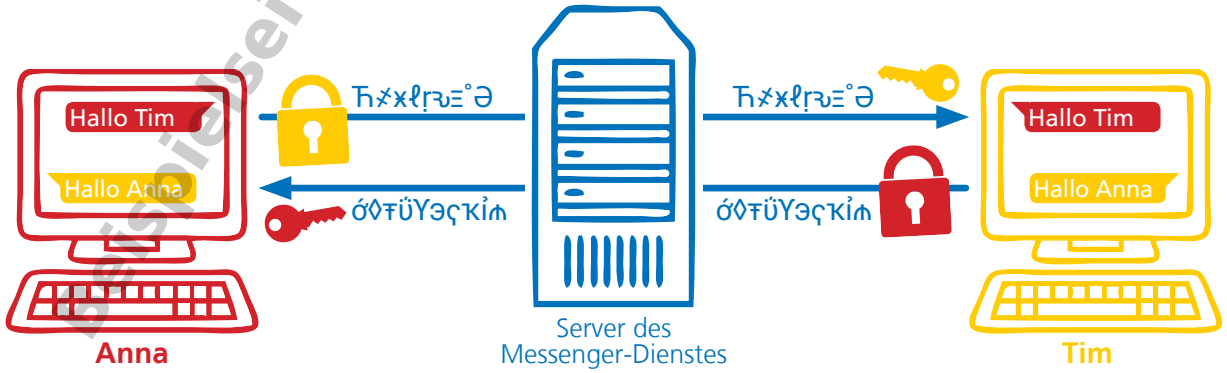
Asymmetrische Verschlüsselungsverfahren benötigen mehr Rechenleistung für das Ver- und Entschlüsseln der Daten, aber sie sind sicherer als symmetrische Verschlüsselungsverfahren. Sie ermöglichen eine sichere Kommunikation im Internet, ohne immense Kosten und Komplexität zu verursachen.

Mit den öffentlichen Schlüsseln können Daten nur verschlüsselt werden. Die öffentlichen Schlüssel aller Nutzer und Nutzerinnen eines Messengerdienstes sind in einem Verzeichnis abgelegt, auf das alle Nutzer und Nutzerinnen des Messengerdienstes zugreifen können.

Möchte Anna eine Nachricht an Tim senden, verschlüsselt sie die Nachricht mit dem öffentlichen Schlüssel von Tim. Die Nachricht ist auf dem Weg zu Tim von niemandem zu entziffern. Nur der zu Tims öffentlichem Schlüssel passende private Schlüssel kann die Nachricht entschlüsseln. Die Antwort an Anna verschlüsselt Tim mit Annas öffentlichem Schlüssel. Und nur sie kann mit ihrem privaten Schlüssel Tims Nachricht entschlüsseln.

Da das Ver- und Entschlüsseln nur beim Sender und Empfänger einer Nachricht möglich ist, spricht man von einer Ende-zu-Ende-Verschlüsselung. Beim Austauschen von Nachrichten bemerkt man davon nichts, denn Messengerdienste wie WhatsApp führen das Ver- und Entschlüsseln vollständig ohne unser Zutun durch.

Ende-zu-Ende-Verschlüsselung bei einem Messengerdienst



[1)] https://www.br-online.de/jugend/izi/deutsch/Grundddaten_Jugend_Medien.pdf (Stand Juni 2021)

Ende-zu-Ende-Verschlüsselung

Aufgabe 1
Stell dir vor, ihr würdet in eurer Klasse über einen Messengerdienst symmetrisch verschlüsselte Nachrichten austauschen.

Wie viele unterschiedliche symmetrische Schlüssel wären notwendig, damit jede Schülerin und jeder Schüler mit allen anderen Schülerinnen und Schülern deiner Klasse Nachrichten austauschen kann?

$$\text{Anzahl Schlüssel} = \frac{\text{Nutzer} \times (\text{Nutzer} - 1)}{2}$$

Für eine Klasse mit 24 Schülerinnen und Schülern bedeutet das

$$\text{Anzahl Schlüssel} = \frac{24 \times (24 - 1)}{2} = 276$$

Aufgabe 2
Beschreibe den Ablauf der Ende-zu-Ende-Verschlüsselung bei einem Messengerdienst.

Eine Nachricht von A an B wird mit dem öffentlichen Schlüssel von B verschlüsselt. B kann die Nachricht mit dem eigenen privaten Schlüssel entschlüsseln und lesen.

Die Antwort an A verschlüsselt B entsprechend mit dem öffentlichen Schlüssel von A. A kann die Nachricht mit dem eigenen privaten Schlüssel entschlüsseln und lesen.

Aufgabe 3
Warum kann der Betreiber des Messengerdienstes die auf seinem Server zwischengespeicherten Nachrichten nicht lesen?

Mit dem öffentlichen Schlüssel können Nachrichten nur verschlüsselt werden. Zum Entschlüsseln benötigt man den privaten Schlüssel des Empfängers. Diesen Schlüssel kennt der Betreiber des Messengerdienstes nicht. Daher kann er die auf seinem Server zwischengespeicherten Nachrichten nicht lesen.

Aufgabe 4
Worin besteht der wichtigste Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungen?

Bei einer symmetrischen Verschlüsselung werden alle übertragenen Daten in beiden Richtungen mit ein und demselben Schlüssel ver- und entschlüsselt.
Bei einer asymmetrischen Verschlüsselung werden unterschiedliche Schlüssel für das Ver- und Entschlüsseln der Daten genutzt. Meist handelt es sich dabei um einen öffentlichen und einen privaten Schlüssel.