Verschlüsselung

In Computernetzen können Daten, die zwischen zwei Kommunikationspartnern ausgetauscht werden, mitgelesen werden. Um das zu verhindern, werden die Daten so umgewandelt, dass im Idealfall nur die beiden Kommunikationspartner diese Daten lesen können.
Die Umwandlung der Daten erfolgt mit Hilfe eines Schlüssels, den beide vereinbaren müssen. Dabei wird zwischen zwei Methoden unterschieden:

- Bei **symmetrischen** Verfahren tauschen die Kommunikationspartner den Schlüssel **vorab** aus, so dass der Schlüssel während der betreffenden Sitzung nicht übermittelt wird.
- Bei **asymmetrischen** Verfahren erstellt jeder Kommunikationspartner ein Schlüsselpaar. Ein Schlüssel jedes Schlüsselpaars ist öffentlich, der andere ist geheim.

Wiederholung: Der 'Cäsar-Code'

Angeblich hat der römische Feldherr Julius Cäsar zur geheimen Übermittlung von Nachrichten folgenden **monoalphabetischen Code** verwendet:
Es werden alle Buchstaben im Alphabet um eine feste Anzahl von Stellen verschoben.
Verschiebt man beispielsweise um sieben Stellen, so wird das **A** auf den Buchstaben **H** im 'Cäsar-Code' abgebildet; das **Z** wird dem Buchstaben **G** zugeordnet.

Alphabet wird mit Zuordnungsschlüssel 7 verschlüsselt (codiert)

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

Beispiel: JULIUS CAESAR => QBSPBZ JHLZHY

- Ein lesbarer Text wird mit Hilfe eines Verschlüsselungsverfahrens in eine nicht lesbare Zeichenfolge umgewandelt.

Der 'Cäsar-Code' ist eine einfache Geheimschrift, der Schlüssel ist leicht zu entziffern. Computergestützte Verschlüsselungsverfahren sind viel schwieriger zu „knacken", aber das Prinzip bleibt dasselbe.

Verschlüsselung binär codierter Daten

Beispielsweise im ASCII-Code werden die Buchstaben wie folgt codiert: A -> 065; B-> 066 usw.
Um Zeichen zu verschlüsseln, kann im 'Cäsar-Code' also einfach eine beliebige Zahl *addiert* werden.
Um die Zeichen zu entschlüsseln, wird die Zahl *subtrahiert*.

Wenn man für die Verschlüsselung den jeweiligen Wert eines Buchstabens im ASCII-Code mit dem Schlüssel *multipliziert*, wird es schon schwieriger, den Schlüssel zu knacken als bei der Addition.

- Beispiel: Geheimer Zuordnungsschlüssel (hier: 3)

ASCII-Code wird durch Multiplikation mit Schlüssel 3 codiert

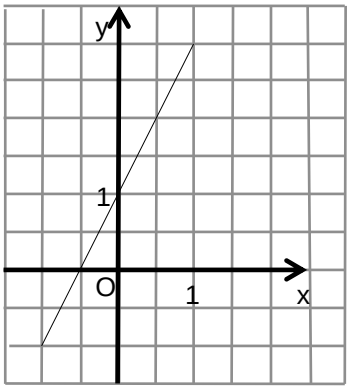
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
195	198	201	204	207	210	213	216	219	222	225	228	231	234	237	240	243	246	249	252	255	258	261	264	267	270

Beispiel: JULIUS CAESAR => 222255228219255249 201195207249195246

1. Codiere anhand dieser Tabelle ein Wort. Notiere aber nur das Ergebnis.

2. Tausche das Ergebnis mit deinem Banknachbarn und entschlüssele dessen Ergebnis.

- Mathematisch vereinbart man damit eine Funktion. Ein Computer kann Daten mit einer mathematischen Funktion einfach verschlüsseln, weil die Daten binär codiert vorliegen, z. B. im ASCII-Code:



Zeichen	A	B	C	…	Z
ASCII-Wert dezimal	065	066	067		090

Auszug aus der ASCII-Tabelle

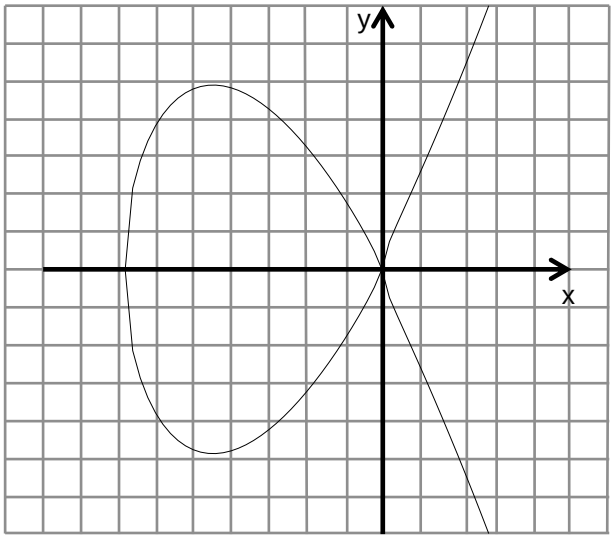
Für das nachfolgende Experiment wird nur der Ausschnitt von A (065) bis Z (090) verwendet. Wenn du z. B. „A“ verschlüsselst, führt das zu dem Ergebnis 2 · 65 + 1 = 131, also dem Zeichen ƒ.
Für den Buchstabe I gilt: 2 · 73 + 1 = 147, also das Zeichen “ (Anführungszeichen links oben).
Hinweis: Auf der nächsten Seite befindet sich ein Auszug aus der ASCII-Tabelle.

3. Gegeben ist die Funktion y = 2x + 1.
   - Der Funktionsgraf ist in dem Koordinatensystem oben eingezeichnet.
   - Gegeben ist die codierte Kurznachricht ‡Ÿ‰‹. Entschlüssele die Nachricht.

Codierte Kurznachricht:	‡	Ÿ	‰	‹
ASCII-Wert der codierten Kurznachricht				
Uncodierte Kurznachricht:				

Ergebnis:

- Die Wissenschaft, die sich mit Informationssicherheit befasst, also u. a. mit der *Verschlüsselung* von Informationen, nennt man **Kryptographie**.
  Das *Entschlüsseln* von Informationen bezeichnet man als **knacken**.



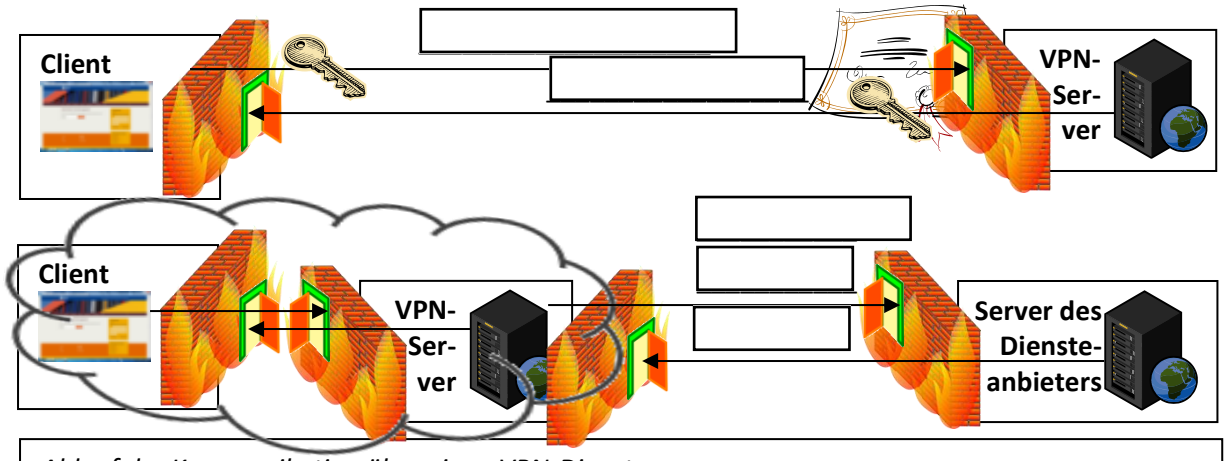
Den „Cäsar-Code“ kann man recht einfach knacken. Deshalb werden aufwändigere mathematische Verfahren verwendet. Aktueller technischer Stand sind elliptische Kurven, für deren Entschlüsselung man Logarithmen benötigt. (Stand: September 2017)
Ein einfaches Beispiel wäre die Funktion $y^2 = x^3 + 4x^2 + x$, die zu dem Grafen rechts führt.

4. Informiere dich im Internet über Verschlüsselung bei Kurznachrichtendiensten. Suche bei dem Dienst, den du nutzt. Überprüfe die Angaben auch in unabhängigen Quellen.
   Wenn du keinen Kurznachrichtendienst nutzt, wähle einen beliebigen Dienst.

ASCII-Wert	Zeichen	Erklärung					
065	A		109	m	153	™	Trademark
066	B		110	n	154	š	
067	C		111	o	155	›	Größer
068	D		112	p	156	œ	kleines OE
069	E		113	q	157	•	
070	F		114	r	158	ž	
071	G		115	s	159	Ÿ	großer Y-Umlaut
072	H		116	t	160		spezielles Leerzeichen
073	I		117	u	161	¡	umgekehrtes Ausrufezeichen
074	J		118	v	162	¢	Cent
075	K		119	w	163	£	Pfund
076	L		120	x	164	¤	Währung
077	M		121	y	165	¥	Yen
078	N		122	z	166	¦	unterbrochener Strich
079	O		123	{	167	§	Paragraph
080	P		124	|	168	¨	Umlautpunkte
081	Q		125	}	169	©	Copyright
082	R		126	~	170	ª	weibliches Ordinal
083	S		127	□	171	«	franz. Anführung links
084	T		128	€	172	¬	Nicht
085	U		129	•	173		leichter Gedankenstrich
086	V		130	‚	174	®	registriertes Trademark
087	W		131	ƒ	175	¯	Makrone
088	X		132	„	176	°	Grad
089	Y		133	…	177	±	Plusminus
090	Z		134	†	178	²	hochgestellte 2
091	[	eckige Klammer auf	135	‡	179	³	hochgestellte 3
092	\	Backslash	136	ˆ	180	´	kleines a mit Akzent
093	]	eckige Klammer zu	137	‰	181	µ	My
094	^	Potenz	138	Š	182	¶	Paragraph
095	_	Unterstrich	139	‹	183	·	mittlerer Punkt
096	`	Akzent	140	Œ	184	¸	Cedilla
097	a		141	•	185	¹	hochgestellte 1
098	b		142	Ž	186	º	männliches Ordinal
099	c		143	•	187	»	franz. Anführung rechts
100	d		144	•	188	¼	Bruch 1/4
101	e		145	‘	189	½	Bruch 1/2
102	f		146	’	190	¾	Bruch 3/4
103	g		147	“	191	¿	umgekehrtes Fragezeichen
104	h		148	”	192	À	großes A mit Akzent
105	i		149	•	193	Á	großes A mit Akzent
106	j		150	–	194	Â	großes A mit Zirkumsflex
107	k		151	—	195	Ã	großes A mit Tilde
108	l		152	˜	196	Ä	großer A-Umlaut

VPN (Virtuelles privates Netzwerk)

5. Ergänze die Beschriftung in der Grafik:



Ablauf der Kommunikation über einen VPN-Dienst:
- *Der Client und der VPN-Server authentifizieren sich und tauschen Schlüssel aus.*
- *Ab sofort befinden sich Client und Server in einem virtuellen privaten Netzwerk.*
- *Danach sendet der Client Daten verschlüsselt an den VPN-Server.*
- *Der VPN-Server vergibt eine neue IP-Adresse und sendet die Daten an den Diensteanbieter. Dadurch ist die ursprüngliche IP-Adresse des Clients außen nicht mehr nachvollziehbar.*
- *Der Diensteanbieter sendet Daten an den VPN-Server, die dieser an den Client weiterleitet. Die Verbindung kann nur bis zum VPN-Anbieter zurückverfolgt werden.*

6. Beschaffe Informationen zu Preisen und Verschlüsselungsverfahren verschiedener Diensteanbieter. Notiere die Informationen und überprüfe die Angaben mit Hilfe unabhängiger Quellen.
   - VPN-Dienst *(für alle Beispiele gilt Stand: September 2017)*
   - E-Mail-Dienst
   - Kurznachrichtendienst

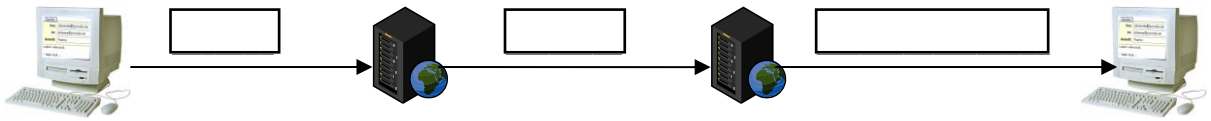
➢ **Vermeide** Experimente wie beispielsweise die Nutzung des **Tor**-Netzwerks oder Zugänge zu Servern mit der inoffiziellen **Darknet**-Endung .onion! Richtig ist, dass hier eine **Anonymisierung** möglich ist, weil die IP-Adresse ähnlich wie bei VPN-Verbindungen durch Weiterleitung verschleiert wird. Als Darknet wird oft der Teil des Internets gesehen, in dem man illegale Waren einkaufen kann, z. B. Falschgeld, Waffen, Kredit- und Debit-Karten, Malware oder Accountdaten.
Um die **Ende-zu-Ende-Verschlüsselung muss man sich aber selbst kümmern**. Auch gibt es keinerlei Regulierung innerhalb dieser Netzwerke. Vielmehr betreiben Kriminelle und höchstwahrscheinlich auch Geheimdienste eigene Knoten, um Angriffe auf die Clients zu starten oder Daten wie Zugänge zu Nutzeraccounts abzuschöpfen.
Die Möglichkeiten der Anonymisierung werden also leider durch Kriminelle unter dem Begriff *Darknet* missbraucht. Dabei ist es wichtig, dass sie von möglichst vielen Anwendern genutzt werden, die sich aber aus genannten Gründen mit Sicherheitsfragen auskennen sollten. Grund dafür ist die ursprüngliche Intention der Anonymisierungsnetzwerke, nämlich Schutz zu bieten, beispielsweise für Menschenrechtsaktivisten, die in ihren Heimatländern politisch verfolgt werden.

Authentifizierung und Verschlüsselung von E-Mails

Hier sollen die Wege für den Versand und die Speicherung von E-Mails genauer betrachtet werden.

- Der Versand mit einem E-Mail Client erfolgt mit dem Protokoll SMTP. Beim Empfang mit POP werden die E-Mails lokal gespeichert und beim Provider gelöscht; mit IMAP können die E-Mails zusätzlich auch noch beim Provider belassen werden, um von überall her Zugriff auf die E-Mails zu haben.

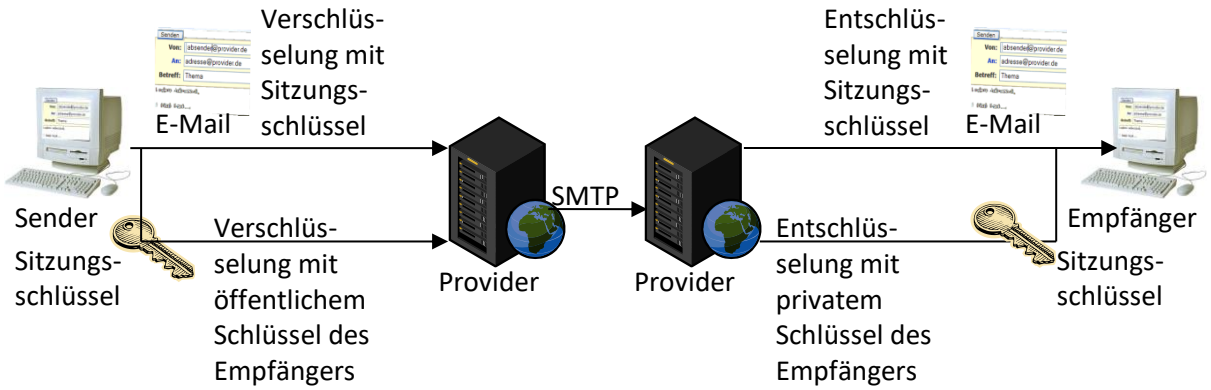
7. Ergänze die verwendeten Protokolle auf den Pfeilen für den Versandweg.



Weg einer unverschlüsselten E-Mail mit verwendeten Protokollen

Für eine Ende-zu-Ende-Verschlüsselung ist (Open-) PGP (Pretty Good Privacy) eine geeignete Wahl (Stand September 2017). Metadaten (Absender und Empfänger) können zwar weiterhin aufgezeichnet werden, der Inhalt bleibt aber geheim. Allerdings müssen alle Kommunikationspartner ein Tool für PGP installieren (am PC z. B. Gpg4win). Die Verwendung erfordert also etwas Aufwand.
Ähnlich wie bei RSA werden auch bei PGP Schlüsselpaare verwendet: Auf dem Rechner des Nutzers wird ein öffentlicher und ein passwortgeschützter privaten Schlüssel erstellt. PGP hat damit denselben Schwachpunkt wie RSA: Wenn ein Dritter einen privaten Schlüssel erhält, kann er im Nachhinein alle Kommunikationsvorgänge entschlüsseln, die damit im Zusammenhang stehen. Außerdem gibt es keine zentralen Zertifizierungsstellen, die Benutzer müssen sich gegenseitig vertrauen.
Die Einrichtung der PGP-Verschlüsselung läuft folgendermaßen ab:

- Jeder Kommunikationspartner erzeugt ein Schlüsselpaar. Dazu gehört ein Widerrufszertifikat, mit dem sich der PGP-Schlüssel als ungültig markieren lässt. Das ist nötig, wenn der Schlüssel gehackt wurde oder der Nutzer das Passwort vergessen hat.
- Dann wird der öffentliche Schlüssel mit einer digitalen Signatur versehen („beglaubigt“), die mit dem privaten Schlüssel verschlüsselt und nur mit dem öffentlichen Schlüssel entschlüsselt werden kann. Dadurch wird die Zugehörigkeit des öffentlichen Schlüssels zu dem Besitzer gewährleistet.
- Jetzt kann man den öffentlichen Schlüssel an E-Mails anhängen oder auf Keyservern speichern.
- Zum Versand einer E-Mail erzeugt der Absender einen Sitzungsschlüssel und verschlüsselt ihn mit dem öffentlichen Schlüssel des Empfängers. Der Sitzungsschlüssel kann damit nur mit dem privaten Schlüssel des Empfängers entschlüsselt werden.



Mit PGP verschlüsselte E-Mail

- Bei Verwendung von Webmail-Frontends ist die Kommunikation vom PC zum Provider durch eine verschlüsselte Verbindung des Browsers abgedeckt.
  Allerdings muss man dem Provider großes Vertrauen entgegenbringen:
  Erstens müssen die gespeicherten E-Mails gegen fremde Zugriffe geschützt werden und zweitens müssen die Provider untereinander E-Mails verschlüsselt austauschen.

Die großen deutschen E-Mail Provider, die mit „E-Mail made in Germany“ werben, haben unverschlüsselte Zugänge abgeschaltet. Der verschlüsselte Transport von E-Mails im Internet ist aber auch hier trotzdem nicht sicher, weil nicht alle Firmen, Behörden und private Betreiber über genügend Zeit und Know-How verfügen, um das zu gewährleisten. Auch werden bekannt werdende Sicherheitslücken eher bei großen Anbietern schneller und zuverlässiger geschlossen. Im Normalfall ist man bei einem professionellen E-Mail-Dienst auf der sichereren Seite als bei einem solchen, der von interessierten Laien administriert wird.

Wenn man seinem E-Mail Provider vertrauen möchte, ist das Anlegen eines Zertifikats mit einem Schlüsselpaar recht einfach. Das könnte innerhalb eines Webmail-Accounts so aussehen:

Digitales Zertifikat

Hier wird Ihnen das Zertifikat Ihres Postfachs angezeigt. Darüber hinaus können Sie hier Ihr Zertifikat exportieren: Falls Sie mit einem E-Mail-Programm arbeiten, können Sie Ihr Zertifikat auf Ihrem Computer abspeichern und in das gewünschte Programm importieren.

Ausgestellt für:
E-Mail-Adresse@provider.xx

Ausgestellt von:

Provider TrustCenter E-Mail-Zertifikate

Seriennummer: 73067531

Gültig von . .20 bis . .20

Fingerprint: 1d9ff76ff2344c8329fa7722c7b5fb8d

Public Key:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCHCAsxOApp/gcfEm52duVhTesl
4HjK/wWY Fxg4d3vxrf/hCquFi80eSBrR6FNqx65TueDGr6wKBxmLRgPkXHBYKkx
SMMG9MSAxhlU/3OquzMTueIu1 AxEQ8ZqPqw U Db Qu36gvANY8Du5yDQnuySrZ
KfikBWts5SWweY6/0QIDAQAB
-----END PUBLIC KEY-----
```

So verwenden Sie Ihr Zertifikat in einem E-Mail-Programm:

1. Schritt: Legen Sie ein Kennwort für den privaten Schlüssel fest.

Kennwort:

Kennwort wiederholen:

2. Schritt: Speichern Sie das Zertifikat auf Ihrem Computer.

Zertifikat exportieren

3. Schritt: Importieren Sie das Zertifikat in Ihr E-Mail-Programm.

Das Rootzertifikat können Sie im TrustCenter herunterladen.

Beispiel für ein E-Mail Zertifikat (Quelle: web.de)

Hier muss man abwägen, ob ein auf dem eigenen PC gespeicherter Schlüssel sicherer ist als ein bei einem Provider gespeicherter Schlüssel. Dienstanbieter müssen Daten auf richterlichen Beschluss herausgeben. Auch können Daten durch einen Angriff von Kriminellen bzw. von Geheimdiensten entwendet werden. Dasselbe gilt auch für den eigenen PC und für Server, die in Eigenregie gepflegt werden.