ZPG IMP – Klasse 8

Informationsgesellschaft und Datensicherheit

Unterrichtsverlauf

Miriam Klein – E-Mail: miriam.Klein@web.de. – April 2018

1 Inhaltsverzeichnis

1 Übersicht

In der ersten Stunde wird zunächst motiviert, warum Datensicherheit bzw. Kryptologie wichtig ist.

In den folgenden Stunden werden die kryptographischen Verfahren betrachtet. Die Betrachtung der Verfahren in historischer Reihenfolge hat den Vorteil, dass man zunächst auf ein Verfahren eingeht: *Wie wird ver- und entschlüsselt?* Anschließend betrachtet man den kryptoanalytischen Askpekt des Verfahrens: W*ie kann man das Verfahren knacken?* Das führt dann unmittelbar zu der Frage: *Wie kann man das Verfahren verbessern?*

Angefangen von der Skytale als Beispiel für ein Transpositionsverfahren, gelangt man über das aus Klasse 7 bekannte Cäsar-Verfahren zum Vigenère-Verfahren und zum absolut sicheren One-Time-Pad. Als modernes (symmetrisches) Verfahren wird das AES-Verfahren (Advanced Encryption Standard) vorgestellt.

Das Kerckhoffs'sche Prinzip wird anschließend behandelt, kann aber je nach Zeit oder Anlass auch vorgezogen werden.

Die kennengelernten Verfahren werden im Anschluss strukturiert und verglichen bezüglich ihrer Eigenschaften: symmetrisch, Transposition, Substitution, monoalphabetisch, polyalphabetisch.

Anschließend verschlüsseln die Schülerinnen und Schüler (SuS) ihre eigenen Daten, beispielsweise ihren Stick mit VeraCrypt.

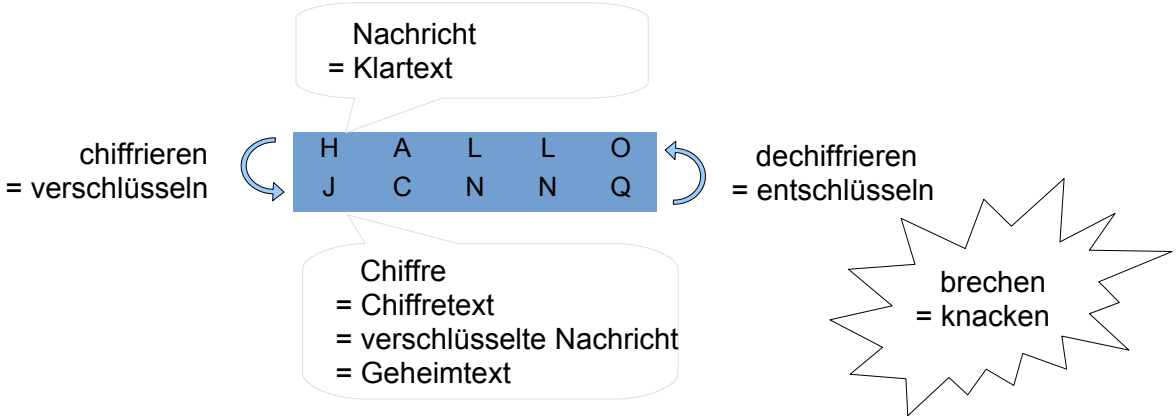
Abschließend wird das Sammeln personenbezogener Daten betrachtet, und er werden Möglichkeiten aufgezeigt, eben dieses einzuschränken.

1 Korrekte Verwendung der Begriffe

Umgangssprachlich werden kryptologische Begriffe oft nicht eindeutig verwendet. Daher ist in besonderem Maße auf eine korrekte Verwendung der Begriffe zu achten. Hier eine kurze Zusammenfassung:

Beim **Datenschutz** wird die Person mit ihren Rechten geschützt (Persönlichkeitsrecht, Urheberrecht,...).

Bei der **Datensicherheit** werden die Daten vor unberechtigten Zugriffen geschützt.



Die **Kryptologie** umfasst die Kryptographie und die Kryptoanalyse.

Bei der **Kryptographie** geht es um das Verschlüsseln und das Entschlüsseln von Nachrichten

mit einem Schlüssel.

Bei der **Kryptoanalyse** geht es um das Brechen bzw. Knacken der Chiffre, ohne den Schlüssel zu kennen.

Bei einer **Verschlüsselung** ist das Verfahren (meist) bekannt, der Schlüssel ist geheim. Es geht um den Austausch von Informationen, die nicht für alle bestimmt sind..

Bei einer **Codierung** ist das Verfahren bekannt, und die Anleitung zum Codieren und Decodieren öffentlich. Einen Schlüssel gibt es nicht, und die ausgetauschten Informationen sind nicht geheim. Beispiele hierzu kennen die Schülerinnen und Schüler aus Klasse 7 (Blindenschrift, Morsecode, …).

2 Differenzierung

Zur aktuellen Stunde passende Differenzierungsmöglichkeiten finden sich direkt bei der Beschreibung der Unterrichtsstunde.

Zusätzlich kann folgendes Material bereitgehalten werden, und bei Bedarf eingesetzt werden:

- Das **Spioncamp** der Uni Wuppertal[1] besteht aus einzelnen Stationen, die voneinander unabhängig bearbeitet werden können. Dazu einfach die pdf-Datei ausdrucken und ggf. laminieren.
  - Transposition: (a) Schablonen (b) Pflügen
  - Substitution: (a) Freimaurer (b) Playfair (c) Rotoren
- Auf den Seiten von **MysteryTwister**[2] finden sich verschiedene Challenges, die auch ohne Anmeldung bearbeitet werden können – z.T. auch ohne Rechner. Es eignen sich z.B.:
  - Fleissner-Schablone[3]
  - Biber-Code[4]
  - Schneewittchen und die sieben Zwerge[5]

3 Weitere hilfreiche Links

- inf-schule[6]
- Cryptool[7]
- Krypto-im-Advent[8]

1 https://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf (Abgerufen am 15.4.18)
2 https://www.mysterytwisterc3.org (alle mysterytwisterc3-Seiten abgerufen am 15.4.18)
3 https://www.mysterytwisterc3.org/images/challenges/mtc3-meier-01-fleissner-de.pdf
4 https://www.mysterytwisterc3.org/images/challenges/mtc3-meier-04-biber-de.pdf
5 https://www.mysterytwisterc3.org/images/challenges/mtc3-meier-05-snow-de.pdf
6 *https://www.inf-schule.de/* (Abgerufen am 8.5.18)
7 *https://www.cryptool.org/de/* (Abgerufen am 8.5.18)
8 *https://www.Krypto-im-Advent.de* (Abgerufen am 8.5.18)

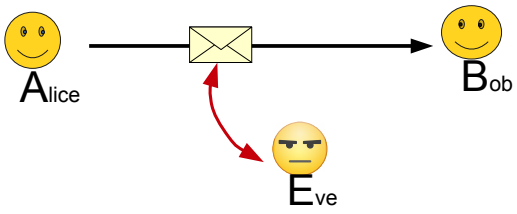
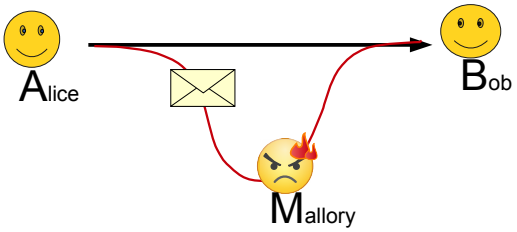
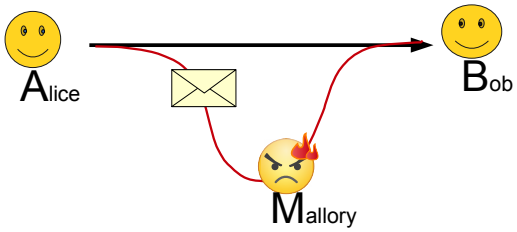
2 Datensicherheit – wozu?

Einstiegsspiel:

Der Lehrer schreibt etwas auf einen Zettel, faltet ihn und schreibt den Namen einer weiter entfernt sitzenden Schülerin oder Schülers darauf. Er bittet eine andere Schülerin oder Schüler, den Zettel an den Adressaten weiterzuleiten.

Je nach Lerngruppe wird beobachtet und besprochen, was passiert ist und/oder besprochen was alles hätte passieren können.

Es lassen sich damit schnell die Angriffsszenarien und die entsprechenden Ziele der Kryptologie herausarbeiten.

Szenarien:	**Gefahren:**	**Ziele** der Kryptologie
	**mitlesen**	=> **Vertraulichkeit** Können wirklich nur Alice und Bob die Nachricht lesen?
	**ändern**	=> **Integrität** Ist die Nachricht unverändert? Sind die Daten original?
	**als A ausgeben**	=> **Authentizität** Kommt die Nachricht wirklich von Alice? Landet die Nachricht wirklich bei Bob? => **Verbindlichkeit** Kann Bob beweisen, dass die Nachricht von Alice kommt, selbst wenn sie es abstreitet? ('*Habe ich nie gesagt*.') Kann Alice beweisen, dass Bob die Nachricht erhalten hat? ('*Habe ich nicht bekommen*.')

=> Unterschiedliche **Ziele** erfordern unterschiedliche **Verfahren**.

Bsp.: Eine Verschlüsselung liefert Vertraulichkeit, aber keine Authentizität.

Wie können die **Ziele erreicht** werden?

	Schutz in der analogen Welt bietet z.B.:	**Schutz** in der **digitalen** Welt bietet z.B.:
Vertraulichkeit	Tresor	E-Mails verschlüsseln Daten verschlüsseln
Integrität	Dokumentenechte Tinte, Hinterlegung beim Notar, Tresor, versiegelter Umschlag	Digitale Signatur
Authentizität	Personalausweis, Unterschrift	Passwort Zugangskontrolle Digitale Signatur
Verbindlichkeit	(vom Notar beglaubigte) Unterschrift	Digitale Signatur

Die SuS sehen oft keine Notwendigkeit, ihre eigenen Daten zu schützen. Man kann die Motivation erhöhen, indem Fallbeispiele mit Lebensweltbezug durchgespielt werden.

Beispiele: Ein ungesichertes Handy oder ein USB-Stick werden vergessen, jemand erhält eine E-Mail, die nicht für ihn bestimmt ist, jemand hat Zugriff auf einen fremden Rechner-Account.

Material:

01_iud_ab_DatensicherheitWozu.odt

DATENSICHERHEIT

Datensicherheit – Wozu?

Bearbeite folgenden Fall und beschreibe, wie der Fall weitergehen könnte.

Fall A:

Lina hat immer einen USB-Stick bei sich, auf dem sie alles speichert, was sie so brauchen könnte:

- *die GFS, die sie nächste Woche halten muss*
- *Fotos: schöne, lustige, peinliche, sehr peinliche*
- *eine Liste ihrer Lieblingssongs*
- *eine lustige Liste mit den Lieblingslehrern und denen, die das nicht sind*
- *eine Liste, in die sie immer ihre Noten einträgt*
- *den Spickzettel für die Bio-Klassenarbeit*
- *ein paar Passwörter, die sie sich nie merken kann*
- *...*

Irgendwie ist ihr der Stick in der Aula abhanden gekommen.

Fall B:

Witzigerweise haben Jan und ein Namensvetter, der auch auf seine Schule geht, beide fast dieselbe E-Mail-Adresse. Manchmal vertippen sich die Leute und Jan erhält eine Mail, die eigentlich für seinen Namensvetter gedacht ist. Diesmal bekommt er diese Mail: „Lieber Jan, sollen wir mal zusammen ins Kino gehen? Da kommt doch gerade dieser lustige Film mit ... Liebe Grüße, Lea"

Fall C:

Einem Lehrer fällt ein USB-Stick aus der Tasche. Sven findet ihn.

Fall D:

Blöderweise lässt Simon sein Handy in der Klasse / Aula / an der Bäckertheke liegen. Max findet es und bemerkt, dass es nicht mit einem Passwort oder ähnlichem geschützt ist.

Fall E:

In den Freistunden dürfen die Schüler und Schülerinnen die Rechner im Computerraum nutzen. Svea möchte an ihrer GFS weiterarbeiten und bemerkt, dass ihre Vorgängerin Vivien vergessen hat, sich abzumelden. Auch ihr Browserfenster ist noch offen. Lisa schaut sich die - äußerst interessante - Browser-Chronik an.

Einer oder mehrere Fälle des Arbeitsblatts können in Gruppen oder auch als vorbereitende Hausaufgabe bearbeitet werden. Das Arbeitsergebnis kann z.B. eine Ideensammlung, ein Rollenspiel oder eine ausformulierte Fortsetzung der Geschichte sein.

Hinweise:

- SuS verwechseln leicht **Zugangskontrolle** (Authentifizierung) und **Verschlüsselung**:

  Bsp.: Das **Passwort** zum **Anmelden am PC** dient der Authentifizierung und ist Bestandteil einer Zugangskontrolle. Das 'Passwort' ist kein Schlüssel. Daten werden dabei nicht verschlüsselt. (Hinweis: Das Passwort muss für die Überprüfung auf dem – zu sichernden - PC gespeichert sein. Das kann zunächst als Widerspruch erscheinen, lässt sich aber leicht erklären, weil Passwörter als Hashwert gespeichert werden. Eine Hashfunktion ist eine nicht-injektive Funktion. Sie ordnet einem Passwort einen Hashwert zu, mit dem man nicht auf das Passwort schließen kann, gleichzeitig aber durch Hashwertbildung eines eingegebenen Wortes prüfen kann, ob dieses das Passwort ist.)

  Bsp: Das **Passwort** bei **VeraCrypt** ist der Schlüssel, mit dem die Daten durch einen Algorithmus verschlüsselt werden. Das 'Passwort', also der **Schlüssel**, ist nirgendwo gespeichert, sondern ist 'Wissen' des Anwenders.

- Eventuell wird es notwendig, auf den Unterschied zwischen **Zugangskontrolle** und **Rechteverwaltung bzw. Berechtigungskonzept** hinzuweisen:

  Die Zugangskontrolle betrachtet die Frage, wer das System betreten darf.

  Das Berechtigungskonzept betrachtet die Frage, **wer** (von denen, die durch Zugangskontrolle authentifiziert sind) auf **welche** Teile des Systems **wie** zugreifen darf (z.B. lesen, schreiben, ausführen,..)

- **2-Faktor-Authentifizierung**:

  Weil zum Beispiel eine Kreditkarte oder TAN-Liste gestohlen werden kann, oder ein Passwort (auf Handy/PC gespeichert) ausspioniert werden kann, nimmt man an, dass es zu unsicher ist, nur **ein** Passwort zu haben. Daher werden zwei Authentifizierungsfaktoren kombiniert und damit das Risiko verringert. Z.B.: Karte und PIN, Passwort und TAN, etc.

Alternativen/Ergänzungen:

- Im klicksave-Modul „*Datensatz - Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind*“ [9] finden sich in Projekt 3 und 4 weitere gute Vorschläge.
- „*Sicherheitsprobleme und Sicherheitsziele*“ in inf-schule.de[10]

9 Klicksave: *https://www.klicksafe.de/service/schule-und-unterricht/klicksafe-to-go/* (Abgerufen am 15.4.18)
10 inf-schule.de: *https://www.inf-schule.de/kommunikation/kryptologie/sicherheitsprobleme* (Abgerufen am 15.4.18)

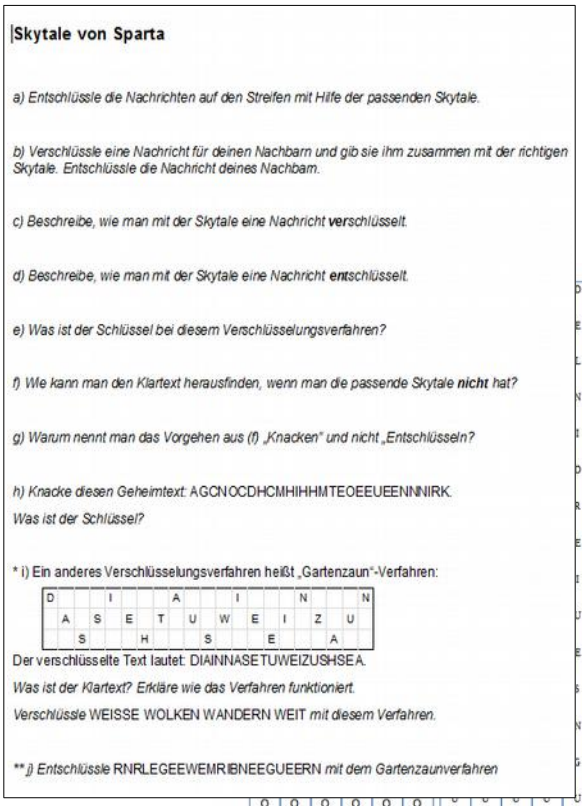
3 Skytale von Sparta

Material:

- mehrere Skytale mit 2-3 verschiedenen Durchmessern (16 mm, 27 mm, Klopapierrolle)

  (Im Baumarkt gibt es passende Rundstäbe.)
- Papierstreifen mit verschlüsselten Nachrichten.

  02_iud_Skytale_Vorlage.pdf
- Leere Papierstreifen zum Verschlüsseln
- *02_iud_ab_skytale.odt*



Skytale von Sparta

a) Entschlüssle die Nachrichten auf den Streifen mit Hilfe der passenden Skytale.

b) Verschlüssle eine Nachricht für deinen Nachbarn und gib sie ihm zusammen mit der richtigen Skytale. Entschlüssle die Nachricht deines Nachbarn.

*c) Beschreibe, wie man mit der Skytale eine Nachricht **verschlüsselt**.*

*d) Beschreibe, wie man mit der Skytale eine Nachricht **entschlüsselt**.*

e) Was ist der Schlüssel bei diesem Verschlüsselungsverfahren?

*f) Wie kann man den Klartext herausfinden, wenn man die passende Skytale **nicht** hat?*

g) Warum nennt man das Vorgehen aus (f) „Knacken" und nicht „Entschlüsseln?

h) Knacke diesen Geheimtext: AGCNOCDHCMHIHHMTEOEEUEENNIRK.
Was ist der Schlüssel?

* i) Ein anderes Verschlüsselungsverfahren heißt „Gartenzaun"-Verfahren:

D			I			A			I			N
	A	S		E	T		U	W		E	I	
			S			H			S			E

Der verschlüsselte Text lautet: DIAINNASETUWEIZUSHSEA.
Was ist der Klartext? Erkläre wie das Verfahren funktioniert.
Verschlüssle WEISSE WOLKEN WANDERN WEIT *mit diesem Verfahren.*

***j) Entschlüssle* RNRLEGEEWEMRIBNEEGUEERN *mit dem Gartenzaunverfahren*

Die SuS bekommen einen Streifen mit dem Geheimtext und mehrere Skytale und versuchen, die Nachrichten auf den Streifen mit Hilfe der passenden Skytale zu entschlüsseln.

Alternativ: Die SuS bekommen je drei verschiedene Textstreifen und drei verschiedene Skytale.

Hinweis: Beim Skytale-Verfahren ist der Schlüssel die entsprechende Skytale bzw. deren Durchmesser. Betrachtet man das Verfahren genauer, kann man als Schlüssel auch die Anzahl der Buchstaben bezeichnen, die einmal um den Stab passen. Dies wird auf den zugehörigen Arbeitsblatt in Teilaufgabe f) deutlich.

Das **Brechen** der Verschlüsselung (Teilaufgabe f)) geschieht durch Simulieren verschiedener Durchmesser. Der Klartext lässt sich durch systematisches Ausprobieren herausfinden:

f) Erster Versuch: Wähle jeden zweiten Buchstaben: (entspricht einer ganz dünnen Skytale)

T	N	F	R	R	U	I	A	E	M	N	U	F	E	D	L	F	L	E	A	E
T		F		R		I		E		N		F		D		F		E		E
	N		R		U		A		M		U		E		L		L		A	

=> Das ergibt keinen Sinn.

=> Nächster Versuch: Jeder dritte Buchstabe:

T	N	F	R	R	U	I	A	E	M	N	U	F	E	D	L	F	L	E	A	E

T			R			I			M			F			L			E		
	N			R			A			N			E			F			A	
		F			U			E			U			D			L			E

=> Das ergibt keinen Sinn.

=> Nächster Versuch: jeder vierte Buchstabe:

T	N	F	R	R	U	I	A	E	M	N	U	F	E	D	L	F	L	E	A	E
T				R				E				F				F				E
	N				U				M				E				L			
		F				I				N				D				E		
			R				A				U				L				A	

=> Das funktioniert. Nachricht: TREFFEN UM ELF IN DER AULA

Differenzierung:

Die Gartenzaunmethode wird als weiteres Verfahren untersucht. Siehe Teilaufgabe i) und j).

Alternativen / Zusatz:

a) Der Geheimtext steht in einer Datei. Durch Ändern der Spaltenbreite können die SuS den Umfang der Skytale simulieren und die Nachricht ablesen.

Umfang (in Buchstaben)	2	3	4	5
Lies spaltenweise von oben nach unten	TN FR RU IA EM NU FE DL FL EA E	TNF RRU IAE MNU FED LFL EAE	TNFR RUIA EMNU FEDL FLEA E ☺	TNFRR UIAEM NUFED LFLEA E

b) Statt der Skytale kann die **Fleißnersche Schablone** als Transpositionsverfahren vorgestellt werden, z. B. als Station des Spioncamp der Uni Wuppertal.[11]

c) Statt der Skytale kann die **Gartenzaunmethode** als Transpositionsverfahren vorgestellt werden. (Siehe dazu die Differenzierungsaufgaben i) und j) auf dem Arbeitsblatt.)

11 *https://ddi.uni-wuppertal.de/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf* (Abgerufen am 6.5.18)

4 Cäsar

Material:

- Die Cäsar-Scheiben bzw. Cäsar-Kronen aus Klasse 7 mitbringen (lassen).

  Ein Exemplar je 2 Schüler.
- *03_iud_ab_Caesar.odt*
- *04_iud_ab_VerbesserungCaesar.odt*

Cäsar-Verfahren

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
Kryptotext	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

Cäsar, Schlüssel **4** (bzw. Schlüssel **E)**

a) Entschlüssle AIMXIV WS *mit dem Schlüssel 4*

b) Verschlüssle ein Wort und gib es deinem Nachbarn zum Entschlüsseln. Nenne dazu auch den Schlüssel.

c) Wie kann man eine Nachricht „knacken"?

d) Wie könnte man das Cäsar-Verfahren verbessern und sicherer machen?

**** e) Mit welchem Schlüssel muss man den Kryptotext* ***ver****schlüsseln, um den Klartext zu erhalten?*

Die SuS wiederholen das bereits aus Klasse 7 bekannte Cäsar-Verfahren (Verschlüsseln, Entschlüsseln, Brechen).

Hinweis:

Schlüssel **4** und Schlüssel **E** sind gleichbedeutend und können alternativ verwendet werden. Schlüssel **4** bedeutet, dass das Kryptotext- Alphabet um **4** nach **links** verschoben wird.

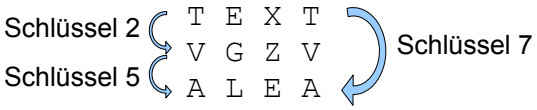
Differenzierung:

Erkennen der Beziehung zwischen Verschlüsseln und Entschlüsseln: Anstatt mit dem Schlüssel 4 zu **ent**schlüsseln, kann man den Chiffretext mit dem Schlüssel 22 **ver**schlüsseln, um den Klartext zu erhalten. (4+22=26)

Wie kann man die Cäsar-Verschlüsselung verbessern? (Teilaufgabe d)

Ziel ist es, zur **polyalphabetischen Verschlüsselung** zu gelangen. Man kann ggf. zuerst andere Ideen der SuS aufgreifen. Hier sind einige Möglichkeiten:

a) Idee: Die Cäsar-Verschlüsselung mehrmals hintereinander ausführen. => Keine Verbesserung!



b) Idee: Ein **Schlüsselwort** unter das Klartextalphabet schreiben, den Rest mit dem ABC auffüllen.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	..
G	**E**	**H**	**E**	**I**	**M**	A	B	C	D	F	J	K	L	..

Brechen: mit einer Häufigkeitsanalyse

c) Idee: **Zufälliger Schüssel** (Substitutionschiffre) (bekannt aus Klasse 7)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	..
X	F	K	E	D	M	A	Q	W	Y	P	M	S	R	.

Brechen: mit einer Häufigkeitsanalyse

(d) Idee: **Homophone Chiffre**, d.h. die Buchstabenhäufigkeiten werden aus-geglichen

Brechen: Die Häufigkeitsanalyse wird schwieriger, ist aber möglich, indem z.B. Muster in Buchstabengruppen identifiziert werden. Bsp: *q* und *u* treten oft gemeinsam auf, und nach *87* folgt meist 72*,67, 19, 99*.

qu: **87**72, **87**67, **87**19, **87**99

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
32	47	65	37	52	91	05	28	02	57	73	43	25	35	51	42	87	97	63	33	72	20	56	80	21	39
59	29	11	76	95	12	36	93	82			2	66	54	23			17	4	86	67					
38		58	46	64		27	45	90			26	24	83	79			41	55	40	19					
68			30	94			88	13				70	34				77	91	96	99					
31				53				85					61				22	18	78						
09				01				14					15				62	71	06						
				92				44					98				08	07							
				48									50												
				60																					
				84																					
				75																					
				68																					
				49																					
				16																					
				74																					

d) Idee: **Mehrere verschiedene Cäsar Schlüssel** anwenden (polyalphabetisch)

→ **Diese Idee wird weiterverfolgt und leitet hin zum Vigenère-Verfahren.**

Sofern die Ideen a) und b) im Unterricht angesprochen wurden, muss der Unterschied herausgearbeitet werden. Zur Erklärung siehe nächster Abschnitt.

Verbesserung des Cäsar-Verfahrens durch Verwenden mehrerer Schlüsselalphabete

Hinweis:

Es ist sinnvoll, diese Übung bzw. das AB **vor** der eigentlichen Vigenère-Verschlüsselung zu machen, damit die SuS ein tieferes Verständnis dafür bekommen, dass die Vigenère-Tabelle nur eine Zusammenstellung aller möglichen Cäsar-Schlüssel ist. Das ist hilfreich, wenn die Vigenère-Verschlüsselung gebrochen werden soll.

04_iud_ab_VerbesserungCaesar.odt

Eine Verbesserung des Cäsar-Verfahrens

Es werden **mehrere** Caesar-Schlüssel immer abwechselnd verwendet.

Beim Schlüsselwort **HUT** benötigt man also die Cäsar-Alphabete H, U und T.

a) Ergänze die Tabelle mit den drei Schlüsselalphabeten.

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
Kryptotext	**H**	I	J	K	L	…																				
Kryptotext	**U**	V	…																							
Kryptotext	**T**	…																								

b) Schreibe das Schlüsselwort unter die Nachricht – so oft wie nötig.

Nachricht	W	I	C	H	T	I	G	
Schlüsselwort								
Verschlüsselte Nachricht								

c) Verschlüssle jetzt die Nachricht.

d) Was fällt dir auf?

Ein Schlüsselwort wird immer wieder hintereinander unter den Klartext geschrieben.

Das entspricht drei **verschiedenen** Schlüsseln: H, U, T

Nachricht	W	I	C	H	T	I	G
Schlüsselwort	**H**	U	T	**H**	U	T	**H**
Verschlüsselte Nachricht	D	C	V	O	N	B	N

Alle Buchstaben, die denselben Schlüsselbuchstaben haben, werden mit derselben Stellung der Cäsar-Scheibe (also demselben Schlüsselalphabet) verschlüsselt !

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
Kryptotext	**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
Kryptotext	**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
Kryptotext	**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

An diesem Beispiel lässt sich gut ablesen, dass Buchstaben, die im Klartext gleich sind, in der verschlüsselten Nachricht unterschiedlich sein können. Bsp.: **I** → C, **I** → B. Außerdem können Buchstaben, die in der verschlüsselten Nachricht gleich sind, im Klartext unterschiedlich sein. Bsp.: T → **N**, G → **N.**

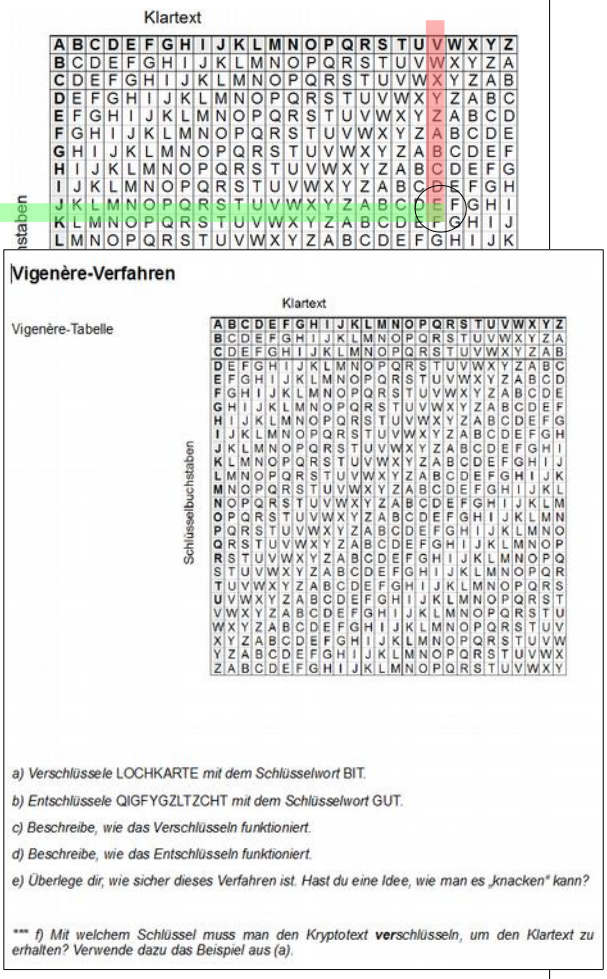
Dieses Verfahren nennt man das **Vigenère**-Verfahren.

5 Vigenère

Material:

- Folie: drucken, Markierungsstreifen abschneiden

  05_iud_Vigenere_Vorlage.pdf
- Cäsar-Scheiben
- *05_iud_ab_Vigenere.odt*



Anstatt wie bisher mit den Cäsar-Scheiben zu verschlüsseln, kann man auch die Vigenère-Tabelle verwenden.

Nach der vorangegangenen Übung ist leicht ersichtlich, dass dieVigenère-Tabelle lediglich eine Zusammenstellung der 26 möglichen Cäsar-Schlüssel ist. Man könnte die Aufgaben auch nur mit der Cäsar-Scheibe lösen.

Verschlüsseln fällt den SuS erfahrungsgemäß leichter als das Entschlüsseln.

Differenzierung:

Erkennen der Beziehung zwischen Verschlüsseln und Entschlüsseln:

Ermittle wie bei Cäsar die „Gegenbuchstaben" des Schlüsselwortes BIT.

B=1	=>	Z=25	weil 1+25=26
I=8	=>	S=18	weil 8+18=26
T=19	=>	H=7	weil 19+7=26

Also **ver**schlüsselt man den Kryptotext mit **ZSH.**

Alternativen / Zusatz:

Die Vigenère-Seiten von inf-schule.de[12]

12 *http://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_vigenere verfahren* (Abgerufen am 6.5.18)

6 Vigenère - Brechen

Man kann das Problem in zwei Teile bzw. Schritte zerlegen:

- Wie lang ist der Schlüssel?
- Wenn die Schlüssellänge bekannt ist, wie kommt man dann auf den Schlüssel?

Hinweis:

Das hier angewendete **Teile-und-herrsche-Prinzip** ist eines der Grundprinzipien in der Informatik:

> Zerlege ein schwieriges Problem in Teilprobleme, die leichter zu lösen sind.

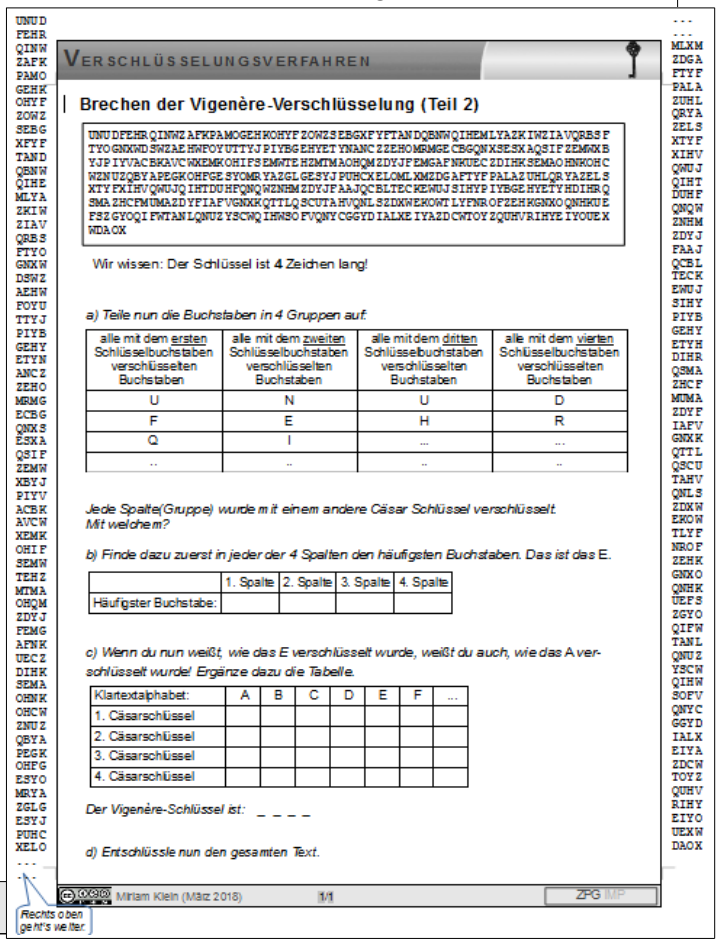
Da der zweite Teil der Problemlösung leichter erscheint, beginnt man damit. Das hat aus didaktischer Sicht Vorteile, man kann aber ebenso mit der Bestimmung der Schlüssellänge beginnen.

Vigenère-Brechen - Schritt 2: Finden des Schlüssels bei bekannter Schlüssellänge

Grundsätzliches Vorgehen:

Annahme: Die **Länge** des Schlüsselworts ist bekannt. Damit ist auch bekannt, welche Buchstaben gleich verschlüsselt werden. Bei einem Schlüsselwort der Länge drei werden also der 1., 4., 7., 10., … Buchstabe mit demselben Cäsar-Schlüssel verschlüsselt. Ebenso der 2., 5., 8., … und der 3., 6., 9., … Buchstabe.

Die Buchstaben werden in so viele Gruppen aufgeteilt, wie der Schlüssel lang ist. Mit einer Häufigkeitsanalyse findet man in jeder Gruppe den häufigsten Buchstaben. Das entspricht (wahrscheinlich) dem 'E' (sofern der Text in Deutsch oder Englisch verfasst ist). Mit der Cäsar-Scheibe findet man nun leicht den Schlüsselbuchstaben für jede Gruppe. Das ergibt das Schlüsselwort.



VERSCHLÜSSELUNGSVERFAHREN

Brechen der Vigenère-Verschlüsselung (Teil 2)

UNUDFEHRQINWZAFKPAMOGEHKOHYFZOWZSEBGKFYFTANDQBNWQIHEMLYAZKIWZIAVQRBSF
TYOGNXWDSWZAEHWFOYUTTYJPIYBGEHYETYNANCZZEHOMRMGECBGQNXSESXAQSIFZEMNXB
YJPIYVACBKAVCMKEMKOHIFSEMWTEHZMTMAOHQMZDYJFEMGAFNKUECZDIHKSEMAOHNKOHC
WZNUZQBYAPEGKOHFGESYOMRYAZGLGESYJPUHCXELOMLXMZDGAFTYFPALAZUHLQRYAZELS
XTYFKIHVQWUJQIHTDUHFQNQWZNHMZDYJFAAJQCBLTECKEWUJSIHYPIYBGEHYETYHDIHRQ
SMAZHCFMUMAZDYFIAFVGNKKQTTLQSCUTAHVQNLSZDKWEKOWTLYFNROFZEHGNXOQNHKUE
FSZGYOQIFWTANLQNUZYSCWQIHWSOFVQNYCGGYDIALKEIYAZDCWTOYZQUHVRIHYEIYOUEX
WDAOX

Wir wissen: Der Schlüssel ist 4 Zeichen lang!

a) Teile nun die Buchstaben in 4 Gruppen auf.

alle mit dem ersten Schlüsselbuchstaben verschlüsselten Buchstaben	alle mit dem zweiten Schlüsselbuchstaben verschlüsselten Buchstaben	alle mit dem dritten Schlüsselbuchstaben verschlüsselten Buchstaben	alle mit dem vierten Schlüsselbuchstaben verschlüsselten Buchstaben
U	N	U	D
F	E	H	R
Q	I	...	...
..	..	..	..

Jede Spalte(Gruppe) wurde mit einem andere Cäsar Schlüssel verschlüsselt. Mit welchem?

b) Finde dazu zuerst in jeder der 4 Spalten den häufigsten Buchstaben. Das ist das E.

	1. Spalte	2. Spalte	3. Spalte	4. Spalte
Häufigster Buchstabe:				

c) Wenn du nun weißt, wie das E verschlüsselt wurde, weißt du auch, wie das A verschlüsselt wurde! Ergänze dazu die Tabelle.

Klartextalphabet:	A	B	C	D	E	F	...
1. Cäsarschlüssel							
2. Cäsarschlüssel							
3. Cäsarschlüssel							
4. Cäsarschlüssel							

Der Vigenère-Schlüssel ist: _ _ _ _

d) Entschlüssle nun den gesamten Text.

Miriam Klein (März 2018) 1/1 ZPG IMP

Rechts oben geht's weiter

Material:

- *06_iud_ab_BrechenTeil2.odt* (ev. die Streifen rechts und links vorher abschneiden)

Die SuS haben auf dem Arbeitsblatt einen Kryptotext und kennen die Schlüssellänge (4). Die Gruppierung der Buchstaben kann von den SuS selber gemacht werden. Alternativ bekommen die SuS die beiden Streifen, links und rechts am Rand des Arbeitsblattes (an den Punkten (...) zusammenkleben.) Jede Spalte entspricht einer Buchstaben-Gruppe. Die SuS zählen arbeitsteilig die Buchstaben in je einer der Spalten (Teilaufgabe a).

Wenn alle vier E's identifiziert wurden, ermittelt man leicht die entsprechenden vier A's. Diese bilden das Schlüsselwort (Teilaufgabe b):

	1. Spalte	2. Spalte	3. Spalte	4. Spalte
Häufigster Buchstabe	Q	E	Y	W

Klartextalphabet	A	B	C	D	E	F	...
1. Cäsarschlüssel	M	N	O	P	Q		
2. Cäsarschlüssel	A	B	C	D	E		
3. Cäsarschlüssel	U	V	W	X	Y		
4. Cäsarschlüssel	S	T	U	V	W		

Vigenère-Schlüssel: MAUS

In Teilaufgabe c) wird nun der Text mit dem gefundenen Schlüsselwort entschlüsselt. Dies kann entweder mit vier Cäsar-Scheiben (arbeitsteilig), mit der Vigenère-Tabelle oder mit CrypTool erfolgen.

Hinweis:

Das Arbeitsblatt kann je nach Gruppe so umgestaltet werden, dass die SuS mehr oder weniger stark geführt werden.

Vigenère-Brechen - Schritt 1: Wie lang ist das Schlüsselwort?

Material:

- *07_iud_ab_BrechenTeil1.odt*

Grundsätzliches Vorgehen: **Kasiski-Test:**

Wenn im Kryptotext eine Buchstabenfolge zweimal auftritt **und** wenn mit ihr dasselbe Wort verschlüsselt wurde, dann ist der Abstand zwischen den beiden Buchstabenfolgen die Schlüssellänge oder ein Vielfaches der Schlüssellänge.

Beispiel1:

```
DASISTDASHAUSVOMNIKOLAUSUNDNICHTDASVOMWEIHNACHTSMANN
TAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGT
WAYBSZWAYAAALVUFNODORTUYNNJGIIATJTSBHMCXINGAIATYFATG
```

Man suche also nach mehrfach vorkommenden Buchstabenfolgen und ermittele den Abstand.

'*DAS*' kommt im Klartext dreimal vor. Im Kryptotext wird daraus zweimal '*WAY*' und einmal '*JTS*'

Der Abstand der beiden '*WAY*'s beträgt 6. 6 = 2 · 3 Der Schlüssel könnte also '2' oder '3' oder '6' Buchstaben lang sein.

'*IAT*' kommt im Kryptotext ebenfalls zweimal vor und hat den Abstand 15. 15 =5 · 3

Brechen der Vigenère-Verschlüsselung (Teil 1)

Wie findet mal die **Schlüssellänge** heraus?

Aufgabe 1: Schlüssel = TAG

Nachricht:	DASISTDASHAUSVOMNIKOLAUSUNDNICHTDASVOMWEIHNACHTSMANN
Schlüssel:	TAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGTAGT
Kryptotext:	WAYBSZWAYAAALVUFNODORTUYNNJGIIATJTSBHMCXINGAIATYFATG

a) Suche im Kryptotext Buchstabenfolgen, die mehrmals vorkommen. Was fällt dir auf?

'3' kommt in beiden Primfaktorzerlegungen vor und könnte die Schlüssellänge sein.

Es ist natürlich möglich, dass die Folgen nur zufällig im Kryptotext gleich sind, im Klartext aber nicht.

Lange Buchstabenfolgen liefern mit größerer Wahrscheinlichkeit richtige Ergebnisse als kurze.

Nachdem das Prinzip erkannt wurde, suchen die SuS in einem längeren Text (Aufgabe 2) nach wiederkehrenden Buchstabenfolgen. Das kann von Hand auf dem Papier erfolgen oder mit Hilfe eines Tools. Erfahrungsgemäß werden auch beim händischen Vorgehen genug Folgen gefunden, um auf die Schlüssellänge schließen zu können.

Aufgabe 2:

WZLQMOPGSVPDMQRXLFPIXZBZXFPCZESXYDLPWTTEDVYDQJEMQMOPLRVBFOZHTP
CZIOKQQMLTHPISYXMWCFYNGIPHTMFDMTEFYMQPVYXPETXUQHDSYZKSPNQPFCBMX
UPQQRJRTGFFTMEIOFHPDVMLQGIPHGREPCZQBWUXWHCIEWFEYGISFHSMODFMREV
UYOPYHFIFCXMWULYSPJNBQFSZNZMDSNYIICMOLBQZQR

a) Suche im Text nach Buchstabenfolgen, die mehrmals vorkommen, und zähle deren Abstand.

b) Zerlege jetzt alle gefundenen Abstände in ihre Primfaktoren.

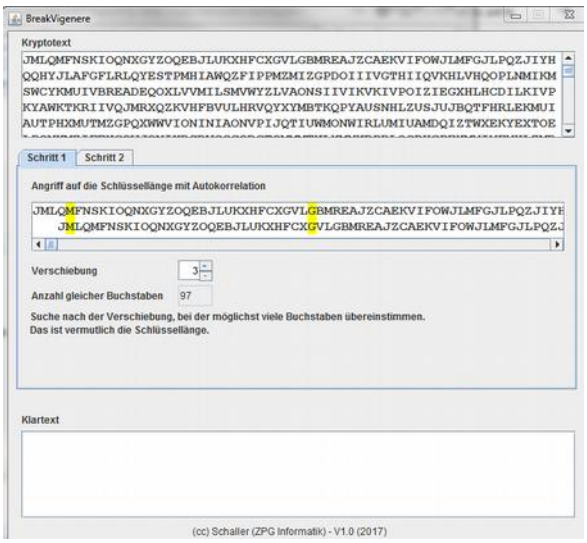
c) Wie lang ist vermutlich die Schlüssellänge?

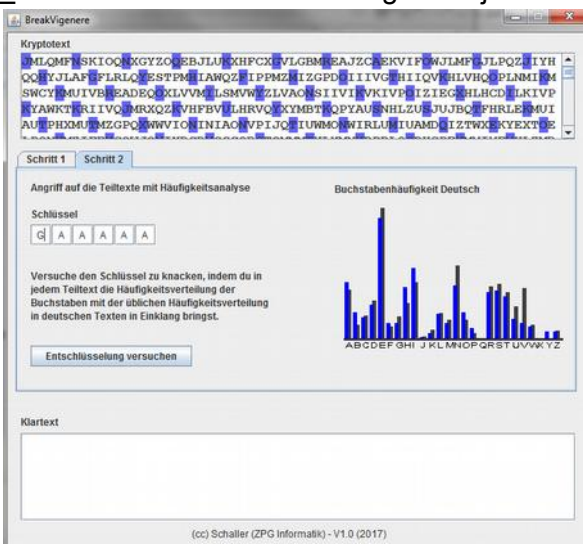
<u>Alternativen / Zusatz</u>

Neben dem händischen Vorgehen kann das Brechen der Vigenère-Verschlüsselung auch mit Hilfe eines Tools erfolgen. Im ZPG-Material befinden sich drei Tools zum Brechen mittels Autokorrelation, mittels Kasiski sowie mittels einer Brute-Force-Methode. Daneben sind auch zwei Tools aus dem Internet erwähnenswert.

Wichtig ist, dass die SuS das Vorgehen verstehen und nicht nur das Tool arbeiten lassen.

- ZPG-Material: 6_software → AngriffVigenere_**Autokorrelation** → BreakVigenere.jar





In Schritt 1 wird der Kryptotext zweimal untereinandergeschrieben und gegeneinander verschoben. Für jede Verschiebung wird vom Tool die Anzahl gleicher Buchstaben angezeigt und zusätzlich im Kryptotext gelb markiert. Die Schlüssellänge ist wahrscheinlich eine Verschiebung, bei der es viele Übereinstimmungen gibt.

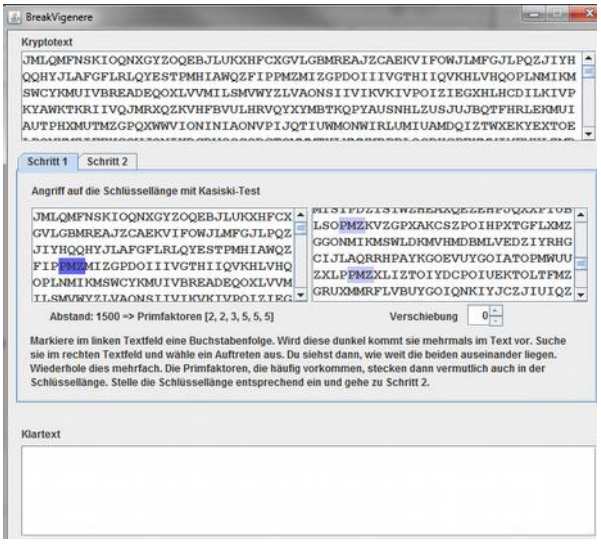
In Schritt 2 wird für jede Buchstabengruppe des Schlüssels ein Diagramm über die Buchstabenhäufigkeit erstellt. Bei deutschen und englischen Texten ist der häufigste Buchstabe wahrscheinlich das verschlüsselte E. Durch Übereinanderlegen der Diagramme erkennt man das verschlüsselte A – den Schlüsselbuchstaben. Hat man alle Schlüsselbuchstaben erraten, lässt man das Tool die Entschlüsselung vornehmen. Der – im besten Fall richtige - Klartext wird angezeigt.

Schritt 2 ist bei allen drei BreakVigenere-Tools gleich.

- ZPG-Material: 6_software → AngriffVigenere_**Kasiski** → BreakVigenere.jar

In Schritt 1 markiert man im kleinen Fenster links eine Buchstabenfolge, von der man vermutet, dass sie im Text häufiger vorkommt. Im kleinen Fenster rechts werden alle Vorkommen der Folge angezeigt. Durch Anklicken wird angezeigt, welchen Abstand die Folge links zur Folge rechts hat, und was die Primfaktoren dieser Zahl sind. Macht man dies mit einigen Buchstabenfolgen und deren Abständen, kann man einen möglichen Schlüssel vermuten und eintragen.

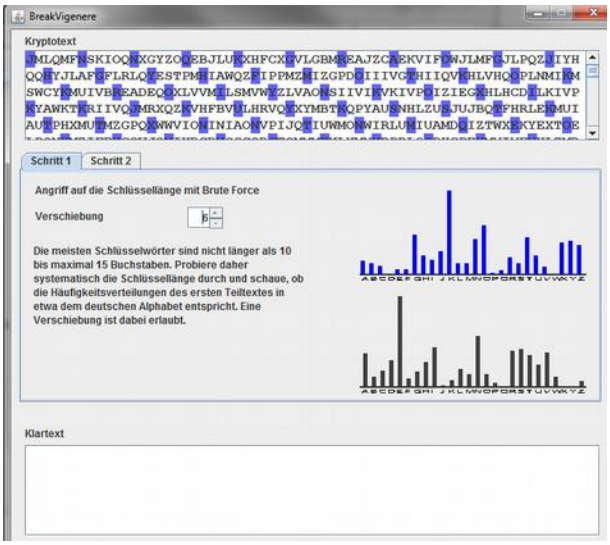
Schritt 2 ist wie beim Autokorrelations-Tool.



- ZPG-Material: 6_software → AngriffVigenere**_partielleBruteForce** → BreakVigenere.jar

  In Schritt 1 wird systematisch jede Schlüssellänge durchprobiert. Jeweils für den ersten Buchstaben des Schlüsselworts wird vom Tool ein Buchstabenhäufigkeitsdiagramm erstellt (oben). Das vergleicht man mit dem Buchstabenhäufigkeitsdiagramm von deutschen Texten (unten). Stimmt es – bis auf eine Verschiebung – überein, hat man die richtige Schlüssellänge gefunden.

  Schritt 2 ist wie beim Autokorrelations-Tool.



- Mit dem Tool auf folgendem Link kann man in einem Text nach wiederkehrenden Buchstabenfolgen der Länge 3 suchen:

  http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/2_Polyalph/kasiski1.html (Abgerufen am 21.4.18)

- Mit dem Tool auf dieser Seite kann man in einem Text nach wiederkehrenden Buchstabenfolgen mit verschiedenen Längen suchen. Es wird auch der ggT angezeigt sowie das Ergebnis der Häufigkeitsanalyse:

  https://www.dominikus-gymnasium.de/kasiski-test.html (Abgerufen am 21.4.18)

Im Material ist ein längerer verschlüsselter Text nebst Schlüssel und Originaltext enthalten. (*07_iud_Text_lang_Brechen.odt*)

Ansonsten erzeugt man Kryptotexte als Beispiele für Schüler einfach mit CrypTool 1[13].

Hinweis:

Da bei der Kasiski-Methode die Abstände in Primfaktoren zerlegt werden, ist es von Vorteil, wenn in IMP-Mathe bereits die Primfaktorzerlegung behandelt wurde (3.1.2.1 Mathematische Grundlagen der Kryptologie).

13 *www.cryptool.org/* (Abgerufen am 21.4.18)

7 One-Time-Pad (OTP)

Material:

- *08_iud_ab_OneTimePad.odt*
- ev. CrypTool 1[14]

Das One-Time-Pad-Verfahren ist ein Vigenère-Verfahren, wobei für den Schlüssel gilt:

- ist mindestens so lang wie die Nachricht
- ist zufällig
- wird nur einmal verwendet
- ist geheim

Ver- und **Entschlüsseln** funktioniert wie beim Vigenère-Verfahren.

Brechen ist nicht möglich! Denn jeder beliebige Text, der genau so lang ist, wie der Kryptotext, könnte der Klartext sein.

Damit ist das OPT ist ein **absolut sicheres** Chiffrierverfahren.

One-Time-Pad (OTP)[1]

a) Der Geheimtext lautet: F O N M Z R

Welcher der folgenden Klartexte könnte mit der Vigenère-Tabelle verschlüsselt worden sein?

T E L L E R, M E S S E R, F E R I E N

Nachricht:

Schlüssel:

Geheimtext: F O N M Z R

b) Denke dir einen längeren Klartext aus (max. 1024 Zeichen). Wähle einen mindestens genauso langen Schlüssel (max. 1024 Zeichen). Verschlüssele deinen Klartext mit dem Vigenère-Verfahren. (z.B. mit CrypTool)

c) Kann deine Sitznachbarin / dein Sitznachbar deinen in (b) erzeugten Geheimtext knacken? Begründe.

Hinweis:

Nachdem alle bisher kennengelernten Verfahren den SuS zunächst meist sicher erschienen und trotzdem alle gebrochen werden konnten, werden die SuS die Sicherheit des OTP zunächst anzweifeln – was durchaus erwünscht ist.

Nachteile:

- Der Schlüssel darf nur einmal verwendet werden.
- Es ist genauso lang wie die Nachricht. Bei der Verschlüsselung eines USB-Sticks z.B. wird ein zweiter Stick benötigt, um den Schlüssel zu speichern.
- Der Schlüssel muss sicher ausgetauscht werden.

14 *https://www.cryptool.org/de/* (Abgerufen am 8.5.18)

Alternativen / Zusatz:

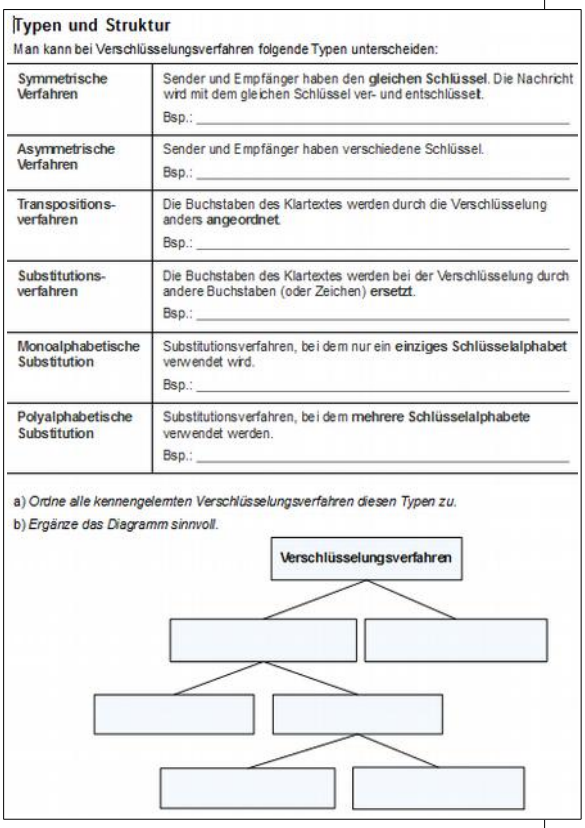
- OTP wurde häufig während des kalten Krieges verwendet. Fotos von OTP-Schlüsseln und Verstecken findet man im Cryptomuseum[15].
- OTP auf inf-schule.de[16]

15 Cryptomuseum: *http://www.cryptomuseum.com/crypto/otp/index.htm* (Abgerufen am 15.4.18)
16 *http://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_onetimepad/version:1* (Abgerufen am 17.4.18)
https://www.inf-schule.de/kommunikation/kryptologie/historischechiffriersysteme/station_sicherheitonetimepad (Abgerufen am 17.4.18)

8 Verschlüsselungsverfahren – Typen und Struktur

Material:

- *09_iud_ab_TypenStruktur.odt*



Typen und Struktur

Man kann bei Verschlüsselungsverfahren folgende Typen unterscheiden:

Symmetrische Verfahren	Sender und Empfänger haben den **gleichen Schlüssel**. Die Nachricht wird mit dem gleichen Schlüssel ver- und entschlüsselt. Bsp.: _____
Asymmetrische Verfahren	Sender und Empfänger haben verschiedene Schlüssel. Bsp.: _____
Transpositions-verfahren	Die Buchstaben des Klartextes werden durch die Verschlüsselung anders **angeordnet**. Bsp.: _____
Substitutions-verfahren	Die Buchstaben des Klartextes werden bei der Verschlüsselung durch andere Buchstaben (oder Zeichen) **ersetzt**. Bsp.: _____
Monoalphabetische Substitution	Substitutionsverfahren, bei dem nur ein **einziges Schlüsselalphabet** verwendet wird. Bsp.: _____
Polyalphabetische Substitution	Substitutionsverfahren, bei dem **mehrere Schlüsselalphabete** verwendet werden. Bsp.: _____

a) *Ordne alle kennengelernten Verschlüsselungsverfahren diesen Typen zu.*

b) *Ergänze das Diagramm sinnvoll.*

Symmetrische Verfahren: Sender und Empfänger haben den **gleichen** Schlüssel. Die Nachricht wird mit dem gleichen Schlüssel ver- und entschlüsselt.

Asymmetrische Verfahren: Sender und Empfänger haben **verschiedene** Schlüssel.

Transpositionsverfahren: Die Buchstaben des Klartextes werden durch die Verschlüsselung anders **angeordnet**.

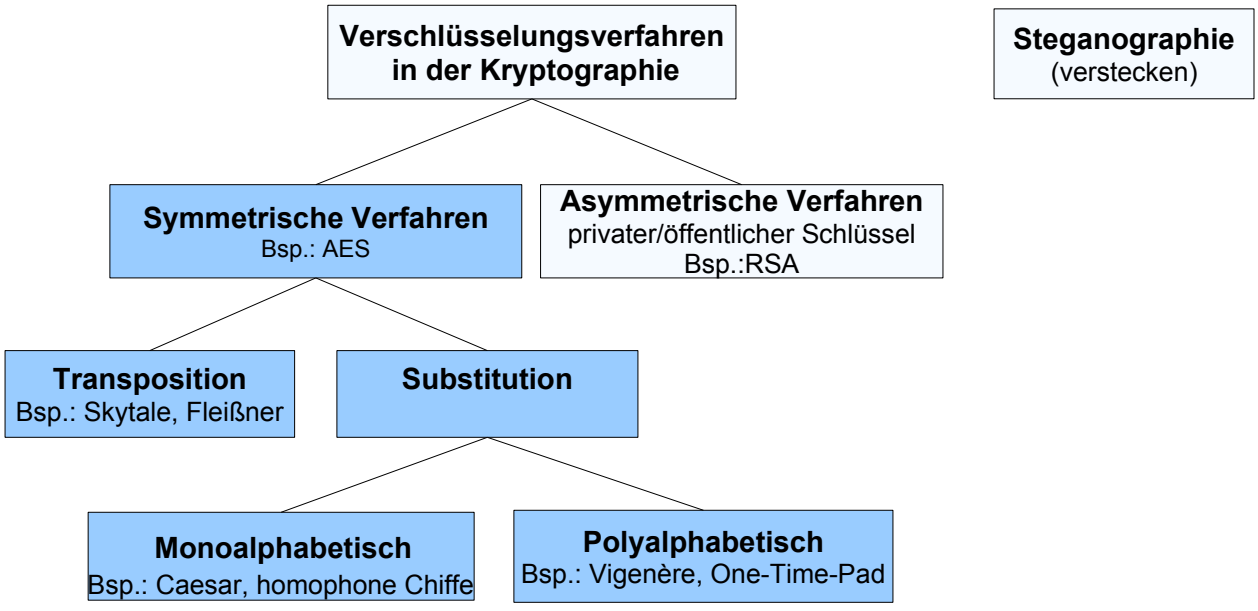
Substitutionsverfahren: Die Buchstaben des Klartextes werden bei der Verschlüsselung durch andere Buchstaben (oder Zeichen) **ersetzt**.

Monoalphabetische Substitution**:**
Substitutionsverfahren, bei dem nur **ein** einziges Schlüsselalphabet verwendet wird.

Polyalphabetische Substitution**:**
Substitutionsverfahren, bei dem **mehrere** Schlüsselalphabete verwendet werden.

Hinweis:

In diesem Zusammenhang kann bei Bedarf auf die Steganographie und die asymmetrischen Verfahren eingegangen werden. Bei der Steganographie werden Informationen nicht verschlüsselt sondern versteckt, weshalb dieses Verfahren i.A. nicht zur Kryptographie gezählt wird.



9 Kerckhoffs' Prinzip

Material:

- *10_iud_ab_Kerckhoffs .odt*

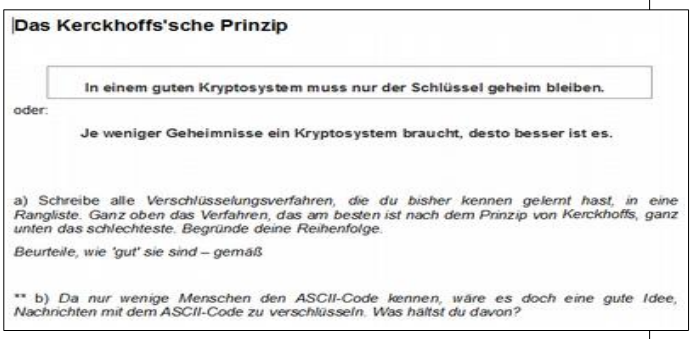
Grundsatz der modernen Kryptologie: Das Kerckhoffs'sche Prinzip (Auguste Kerckhoffs, 1883)

In einem guten Kryptosystem muss nur der Schlüssel geheim bleiben.

Das heißt: Je weniger Geheimnisse ein Kryptosystem braucht, desto robuster ist es.

- 'Gutes' System:
  Nur ein ganz kleiner Teil ist geheim (**Schlüssel**). Das Prinzip ist bekannt.
  Bsp.: Schlüssel + Zylinderschloss
  Vorteil: Jeder kennt das Prinzip, wie ein Zylinderschloss funktioniert, aber nur mit dem konkreten Schlüssel kann man aufschließen.
- 'Schlechtes' System:
  Das **Verfahren** ist geheim.
  Bsp.: Geheimtür hinter oder in einem Schrank
  Nachteil:
  - Jeder muss sich einen eigenen Mechanismus (Verschlüsselungs-verfahren) überlegen.
  - Wenn eine Person den Mechanismus entdeckt hat, muss man eine „neue Tür bauen“, bzw. ein neues Verfahren überlegen.

Die SuS bewerten in Frage a) die bisher kennengelernten Verfahren hinsichtlich ihrer Güte nach dem Kerckhoffs'schen Prinzip.


Das Kerckhoffs'sche Prinzip

In einem guten Kryptosystem muss nur der Schlüssel geheim bleiben.

oder:

Je weniger Geheimnisse ein Kryptosystem braucht, desto besser ist es.

a) Schreibe alle *Verschlüsselungsverfahren, die du bisher kennen gelernt hast, in eine Rangliste. Ganz oben das Verfahren, das am besten ist nach dem Prinzip von Kerckhoffs, ganz unten das schlechteste. Begründe deine Reihenfolge.*

Beurteile, wie 'gut' sie sind – gemäß

** b) *Da nur wenige Menschen den ASCII-Code kennen, wäre es doch eine gute Idee, Nachrichten mit dem ASCII-Code zu verschlüsseln. Was hältst du davon?*

Frage b) kann unterschiedlich tief betrachtet werden:

- Codierungen haben keinen Schlüssel, also sind sie auch keine Verschlüsselungen.
- Wenn aber 'niemand' das Codierungs-Verfahren kennt, dann würden sich Codierungen durchaus zum Verschlüsseln eignen. Allerdings wäre dann das Verfahren an sich der Schlüssel. Sobald nun das Verfahren bekannt wird, kann man es nicht mehr verwenden. Nach Kerckhoffs also ein sehr schlechtes Verfahren. Weil Codierungen derart schlechte 'Verschlüsselungen' sind, werden sie erst gar nicht so genannt .

10 Ein modernes Verschlüsselungsverfahren: AES

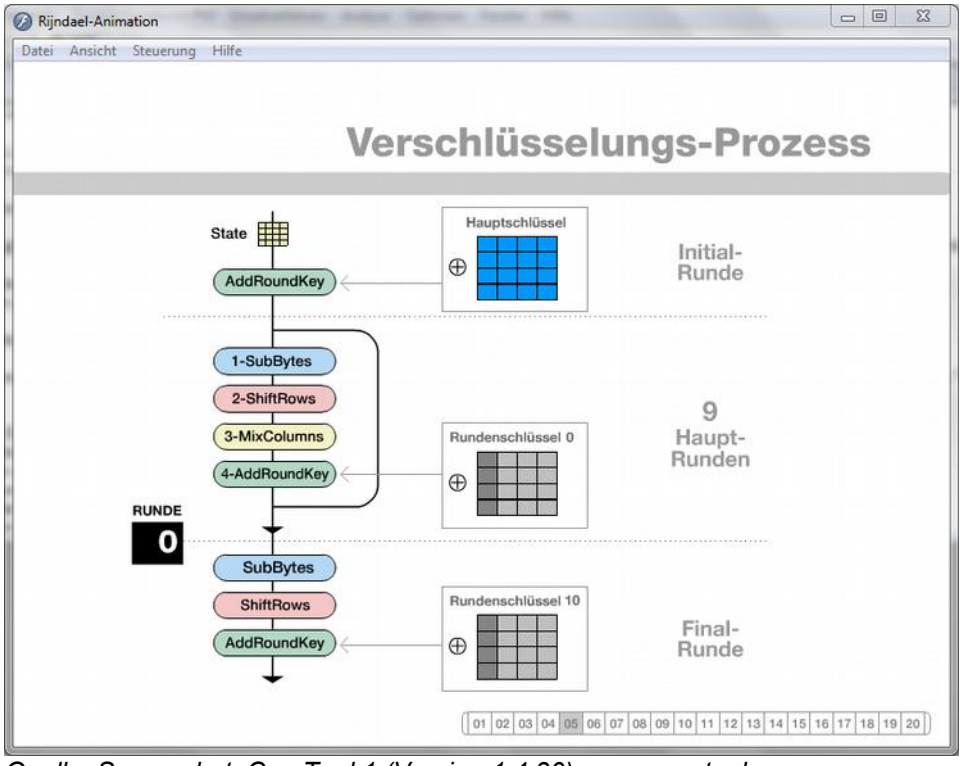
Material:

- CrypTool 1[17]

Das AES-Verfahren (**Advanced Encryption Standard)** ist ein aktuell verwendetes symmetrisches Verfahren. Auch: **Rijndael**-Verfahren oder Rijndael-Algorithmus.

Es wurde von Joan Daemen und Vincent Rijmen entwickelt und im Jahr 2000 vom National Institute of Standards and Technology (NIST) als Standard festgelegt. Es wurde notwendig, weil durch höhere Rechnerleistung bisherige Verschlüsselungsmethoden (z.B. DES) nicht mehr sicher vor Bruteforce-Angriffen waren.

Das Verfahren kann mit Hilfe einer **Animation** innerhalb von **CrypTool 1** visualisiert und den SuS veranschaulicht werden. Dabei werden die einzelnen Runden des Verfahrens durchlaufen und erklärt. Menüpunkt: *Einzelverfahren → Visualisierung von Algorithmen → AES → Rijndael-Animation.*



Quelle: Screenshot: CrypTool 1 (Version 1.4.30), www.cryptool.org

Die CrypTool-Visualisierung wird den SuS vorgeführt und dabei die einzelnen Schritte besprochen.

In Dia 03 sieht man eine Klartextblock (4x4). Beim AES-Verfahren wird der Klartext in mehrere 4x4 Blöcke geschrieben. Jede Zelle ist 1 Byte groß, beinhaltet also genau eine Hexadezimalzahl. Der Schlüssel ist ebenfalls ein 4x4 Block mit Hexadezimalzahlen.

17 *https://www.cryptool.org/de/* (Abgerufen am 8.5.18)

In Dia 05 erkennt man den Prozess der Verschlüsselung, bei dem 11 Runden nacheinander ausgeführt werden (Initial-Runde, 9 Haupt-Runden, Final-Runde).

Dia 06 enthält die vier Verschlüsselungs-Transformationen, die nachfolgend vorgeführt werden.

In **SubBytes** (Dia 07) wird jedes Byte des 'Klartextes' durch ein anderes Byte ersetzt. Das ist eine monoalphabetische Substitution, genau wie z.B. beim Cäsar-Verfahren. Die S-Box entspricht dabei der Cäsar-Scheibe. Hinweis: der Klartext in dieser Runde ist nicht mehr 'klar', weil er in der Initial-Runde bereits verschlüsselt wurde.

In **Shift-Rows** (Dia 08) werden die Bytes zeilenweise rotiert. In jeder Zeile des Klartextblocks werden die Bytes nach links verschoben. Die links 'herausgefallenen' Bytes werden von rechts wieder hinzugefügt. In der zweiten Zeile wird um ein Byte, in der dritten Zeile um zwei Byte und in der vierten Zeile um drei Byte verschoben. Das ist leicht als Transposition erkennbar.

MixColums in Dia 09 ist für die Schüler zu komplex. (Anmerkung: Jede Spalte des Klartextblocks wird mit einer 4x4-Matrix multipliziert (modulo im Galois-Körper mit XOR). Das Ergebnis ist jeweils die veränderte neue Spalte.)

Bei **AddRoundKey** (Dia 10) wird jedes Byte des 'Klartextes' mit dem entsprechenden Byte des Rundenschlüssels mit XOR verknüpft. Allerdings ist XOR laut Bildungsplan erst in Klasse 9 vorgesehen. Daher sollte man Dia 09 und 10 nicht weiter thematisieren.

In Dia 11 sieht man, wie sich der Klartext von Runde zu Runde verändert, bis der Geheimtext entstanden ist.

In Dia 14 bis 20 wird die Generierung der Rundenschlüssel aus dem Hauptschlüssel gezeigt, worauf aber nicht weiter eingegangen werden soll. Es genügt, dass aus dem eigentlichen Schlüssel weitere 10 Schlüssel erzeugt werden, die in Runde 2-11 verwendet werden.

Die Entschlüsselung erfolgt dann analog in umgekehrter Reihenfolge.

Dadurch, dass verschiedene Verschlüsselungsverfahren mehrfach hintereinander ausgeführt werden, bietet das AES ein hohes Maß an Sicherheit, trotz des relativ kurzen Schlüssels von 128 Bit. Das Problem des Schlüsseltauschs ist bei AES, wie bei allen symmetrischen Verfahren, vorhanden, ist aber entschärft durch die Kürze des Schlüssels. Im Vergleich dazu ist OTP zwar sicher, aber nicht prakikabel.

Hinweis:

Da in der CrypTool1-Visualisierung Hexadezimalzahlen verwendet werden, ist es von Vorteil, wenn in IMP-Mathe bereits die Hexadezimalzahlen behandelt wurden (3.1.2.1 Mathematische Grundlagen der Kryptologie).

Zusatz:

Für weitergehende Informationen:

- CrypTool 1
- *https://de.wikipedia.org/wiki/Advanced_Encryption_Standard* (Abgerufen am 4.4.18)

11 Verschlüsselung eigener Daten

Material

- Schüler-Sticks
- *11_iud_VeraCrypt_Anleitung. pdf*
- *VeraCrypt* auf allen Schülerrechnern

Die SuS verschlüsseln ihren Stick oder einen Teil ihres Sticks mit VeraCrypt.

Als Einstieg eignet sich z.B. der Film *Daten Verschlüsseln Einfach Erklärt – 4/5 (4:43)*[18] (Hinweis: Der Film empfiehlt TrueCrypt.)

Im Unterricht werden zunächst gemeinsam die Volumes auf den Schüler-Sticks angelegt. Danach wird VeraCrypt als Hausaufgabe zu Hause installiert, so dass die Volumes auch zu Hause verwendet werden können.

Die Schüleranleitung wurde in verkürzter Form vom Lehrerfortbildungsserver Baden Württemberg übernommen. Weitere Details können dort nachgelesen werden.[19]

Installieren[20] und Einrichten[21] von VeraCrypt, sowie Anlegen[22] und Verwenden[23] eines Volumes.

Hinweis:

Die SuS müssen VeraCrypt zu Hause auf einem Rechner installieren und einrichten. Es empfiehlt sich, im Vorfeld die Eltern durch einen Elternbrief darauf hinzuweisen.

Alternative/Zusatz:

- Verschlüsseln einer Datei bzw. eines Ordners

  (rechter Maus-Klick auf die Datei bzw. den Ordner → Eigenschaften → Allgemein → Erweitert → Inhalt verschlüsseln)
- Erzeugen einer verschlüsselten zip-Datei, um z.B. Fotos oder andere Dateien zu verschicken.[24]

18 *https://www.youtube.com/watch?v=IhoG37uis3k* (Abgerufen am 15.4.18)
19 *Lizenz: CC-BY-NC-SA 3.0 Deutschland. Die Bilder unterliegen der Lizenz CC-BY-NC-ND 3.0 Deutschland*
20 *https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/1install/* (Abgerufen am 13.4.18)
21 *https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/2config/* (Abgerufen am 13.4.18)
22 *https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/3use/index.html* (Abgerufen am 13.4.18)
23 *https://lehrerfortbildung-bw.de/st_digital/medienwerkstatt/dossiers/sicherheit/stickcrypt/vc/4fill/index.html* (Abgerufen am 13.4.18)
24 Hilfreich: *http://www.bitdefender.de/support/erstellen-eines-passwort-geschuetztenzip-archives-363.html* (Abgerufen am 15.4.18)

12 Sammeln personenbezogener Daten

1 Unterrichtsverlauf:

Der Unterrichtsverlauf ist angelehnt an das klicksafe-Modul „*Datensatz – Datenschatz?*“[25] Hier findet man noch weitere Ideen und Ergänzungen.

Einstieg: Aufwerfen der Fragen: *Warum sind Dienste wie WhatsApp kostenlos?*

Wieso sind unsere Daten etwas wert?

Video zu Sensibilisierung: *Nackt im Netz*[26] (ca. 12 min. Ohne den Panorama-Vorspann: von 1:03 bis 11:50) Hier wird gezeigt, welche teilweise kompromittierenden Informationen in URLs stecken.

Optional: Sofern in Klasse 7 noch nicht erfolgt, kann man den Weg einer URL-Anfrage im Internet veranschaulichen, der oft durch mehrere Länder/Kontinente geht, ehe er wieder in Deutschland ankommt. (z.B. mit *traceroute*[27]*)*

Bearbeitung der Frage: *Welche Informationen stecken in einer URL?*
Diese Frage kann gut mit dem Google-Translator[28] veranschaulicht und beantwortet werden oder mit einer Anfrage bei z.B. *booking.com*[29]*.* Im Klicksafe-Modul gibt es ein dazu passendes Arbeitsblatt.

Optional: Demonstration, wie man mit einer IP-Adresse den Standort des Benutzers erfährt.[30] Wie man zusätzlich den Namen und die komplette Adresse erhält, kann man nicht so einfach zeigen.)

Zum Einstieg ins Tracking: Aufwerfen der Fragen:

- *Gestern habe ich nach dem Samsung Galaxy S9 gegoogelt, heute sehe ich immer wieder Werbung für genau dieses Handy – wie kann das sein?*
- *Woher weiß Google, was ich bei Amazon gesucht habe?*

Zum **Veranschaulichen von Tracking** verwendet man *lightbeam*[31]*.* Dieses PlugIn sollte man vorher in Firefox installieren und sich damit vertraut machen. Vor der Vorführung auf 'reset' klicken. Man besucht während der Demo 3-4 Internetseiten (z.B. google, Spiegel-online, web.de, amazon, booking.com) und öffnet dann *lightbeam*. Angezeigt wird: Wie viele Seiten wurden

25 *https://www.klicksafe.de/fileadmin/media/documents/pdf/klicksafe_Materialien/Lehrer_Allgemein/ks_to_go_Datensatz_-_Datenschatz.pdf* (Abgerufen am 8.5.18)
26 *https://www.youtube.com/watch?v=yGXb-ChrSFA* (Abgerufen am 15.4.18)
27 *dnstools.ch/visual-traceroute.html* (Abgerufen am 6.5.18)
28 *https://translate.google.com/* (Abgerufen am 6.5.18)
29 Abgerufen am 6.5.18
30 https://www.maxmind.com/en/geoip2-precision-demo (Abgerufen am 6.5.18)
31 http://www.chip.de/downloads/Firefox-Lightbeam_65106174.html (Abgerufen am 8.5.18)

besucht? Wie viele Anbieter haben eben Informationen über uns erhalten? Als Kreis werden die Anbieter der besuchten Seite dargestellt, als Dreieck weitere Anbieter, die informiert wurden. Es gibt meist auch Dreiecke, die mit mehreren besuchten Seiten verbunden sind.

Diskussion der Frage: *Personalisierte Werbung ist doch super! Oder?*

Hier sollten selbstverständlich beide Seiten betrachtet werden, also nicht nur die Nachteile, sondern auch die Vorteile von personalisierter Werbung.

Die Diskussion kann auch z.B. um „personalisierte Nachrichten“ erweitert werden.

Möglichkeiten, das Sammeln personenbezogener Daten einzuschränken:

Hier gibt es eine Vielzahl von Möglichkeiten, die man den SuS anbieten bzw. vorführen kann.[32]

- **Cookie-Optionen** im Browser: In den Einstellungen kann man sich alle aktuell gespeicherten Cookies anzeigen lassen und ggf. löschen. Man kann einstellen, dass der Browser keine oder alle Cookies annimmt oder dass wird bei jedem Cookie um Erlaubnis gefragt wird. Durch das Abschalten wird die Internetnutzung jedoch unkomfortabler. Sinnvoll: Cookies für Drittanbieter sperren.
- *AdBlock Plus*[33] **blockiert Werbung** im Browser – auch für Smartphone und Tablet.
- *Ghostery*[34] **blockiert Werbung** und zum Teil auch **Tracking**. Zeigt zusätzlich an, welche Werbung und Tracker unterdrückt wurden.
- *'http'* wird unverschlüsselt übertragen, **'https'** hingegen **verschlüsselt**. Auf vielen Seiten ist beides möglich. Das Plugin HTTPS-Everywhere ändert *'http'* automatisch zu *'https'*, sofern möglich. Dazu gibt es auch ein YouTube-Video: *Sicher Surfen mit HTTPS - Einfach Erklärt! - 2/5*[35]
- Bei Apps und Add-ons ist darauf zu **achten**, welche **Berechtigungen** diese verlangen. (Zum Beispiel macht es keinen Sinn, dass eine Taschenlampen-App auf Adressen und Browser-Verlauf zugreifen darf.)
- Statt Google eine **Proxy-Suchmaschine** verwenden. Beispielsweise sucht startpage[36] als Proxy bei Google, und liefert keine Infos an Google.

Wichtig dabei ist, dass Tools keine absolute Sicherheit bieten (es werden z.B. viele Tracker lockiert – aber nicht alle). Zum Teil erlauben Internet-Seiten keinen Zugriff, wenn man Werbung blockiert. Außerdem muss man letztendlich auch den Anbietern dieser Tools vertrauen.

32 Die Ideen stammen zum Teil von klicksafe.de (Modul: Datensatz – Datenschatz?, Abgerufen am 15.4.18) sowie *https://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/vom-web-tracking-zum-app-tracking/teil-3-wie-koennen-sich-nutzerinnen-und-nutzer-selbst-schuetzen/#s|webtracking* (Abgerufen am 15.4.18)

33 *https://adblockplus.org/de/* (Abgerufen am 6.5.18)

34 *https://www.ghostery.com* (Abgerufen am 6.5.18)

35 *https://www.youtube.com/watch?v=tW1-CmggG9s)* (Abgerufen am 15.4.18)

36 *https://www.startpage.com* (Abgerufen am 6.5.18)

2 Hintergrund

a) Wo und wie werden personenbezogene Daten gesammelt?

webtracking:

- **Cookies**: Wenn man eine Internetseite besucht, schickt die Seite eine kleine Datei (das ist ein *Cookie*) mit, die auf dem Computer gespeichert wird. Sie enthält unter anderem eine Nummer, mit der der Benutzer später wieder identifiziert werden kann. Besucht man diese Seite später erneut, muss der Benutzer z.B. seine Adresse nicht erneut eingeben. Über das Cookie „erkennt" die Internetseite den Benutzer und kann so aber auch nach-vollziehen, was er die letzten Male auf der Internetseite angeklickt hat, wofür er sich also interessiert. Die Seite sammelt und speichert Daten über den Benutzer.

  Es gibt persistente Cookies und SessionCookies. Persistente Cookies werden dauerhaft gespeichert, SessionCookies nur für die Dauer einer Sitzung Ursprünglich waren Cookies für den Benutzer hauptsächlich nützlich, mittlerweile haben sehr viele Cookies die Aufgabe, den Benutzer und sein Verhalten nachvollziehbar zu machen bzw. zu tracken.

- **Einbetten** von Elementen auf anderen Seiten: Ein Beispiel ist der „Gefällt mir"-Button von Facebook, der sich auf vielen Seiten wiederfindet. Jedes Mal, wenn eine Seite mit diesem Element angezeigt wird, wird eine Verbindung zu einem Rechner der Firma Facebook Inc. aufgebaut. Dabei dienen Cookies auch dazu, Nutzer wieder zu erkennen. So können Anbieter dann Rückschlüsse darauf ziehen, welche Seiten besucht worden sind. Von diesem Nutzungsverhalten kann dann mittels statistischer Verfahren auf Interessen, Vorlieben und weitere Eigenschaften geschlossen werden."[37]

- **Verknüpfung** der Daten zwischen den verschiedenen Seiten, z.B. mittels **Google-Analytics:**
  Die aufgerufene Seite sendet Informationen an Google-Analytics. Dieses System bündelt die Informationen der Benutzer, die von ganz verschiedenen Seiten übermittelt werden, erstellt Auswertungen und übergibt die Ergebnisse/Analysen den Betreibern der beteiligten Seiten.

- **IP-Adresse und URL**: Bei jedem Seitenaufruf wird die eigene IP-Adresse mitverschickt. Über die IP-Adresse lässt sich der Ort des Benutzers bestimmen (z.B. Karlsruhe), oft auch Name und Adresse. Bei einem Seitenaufruf, werden neben der IP-Adresse auch aufschlussreiche benutzerspezifische Daten innerhalb der URL mitgeschickt. Bei einer Hotel-Buchungsanfrage sind das z.B.: von-/bis-Datum, Ort, Hotel, Anzahl Erwachsener und Kinder). Ähnlich ist es bei einer Flug-Buchungsanfrage. Bei Online-Übersetzern sind teilweise die zu übersetzenden Texte in der URL enthalten. Aus Klasse 7 ist den SuS bereits bekannt, dass eine URL einen Weg über verschiedene Server in verschiedenen Ländern nehmen kann, ehe sie am Ziel ankommt.

b) Wer sammelt diese Daten?

- Bei den erstgenannten Tracking-Varianten sammeln die Betreiber der Internetseiten bzw. ihre Geschäftspartner die Daten.
- Beim Tracking mittels IP und URL kann jeder am Internetverkehr beteiligte Server Daten sammeln.

37 *https://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/vom-web-tracking-zum-app-tracking/teil-1-web-tracking-was-ist-das/#s*|webtracking (Abgerufen am 21.4.18)

- Auch durch (illegale) Hacker-Angriffe können Daten von Firmen-Servern, Cloud-Speichern, etc. gestohlen werden.

c) Warum werden diese Daten gesammelt?

- Benutzerfreundlichkeit: Der Benutzer muss nicht jedes Mal z.B. seine Ausweisnummer bei der Bücherei eintippen. Die Seite „merkt“ sich die Nummer.
- Dem Benutzer wird nur „interessante“ Werbung angezeigt.
- Benutzerverhalten wird erkannt und analysiert: Interessen, Kaufverhalten, Kaufabsichten, Familiensituation (verheiratet, Kinder), (nicht) zurückgezahlte Kredite, ...

  Bedürfnisse der Kunden werden frühzeitig erkannt, z.B. „Kunden die X kaufen, kaufen meist auch Y“.

  Personalisierte Werbung: durch zielgerichtete Werbung werden Marketing-Ausgaben minimiert, der Erfolg (Gewinn) maximiert.
- Weniger Verluste durch nicht-zahlende Kunden: Manche Menschen gelten als weniger kreditwürdig, weil viele Menschen mit ähnlichen Interessen/Verhalten/Namen... ihre Kredite nicht zurückzahlen. Auswirkung: In zuvor noch nie besuchten Onlineshops wird manchen Kunden 'Zahlen per Rechnung' angeboten, anderen nicht.
- Kundenspezifische Preise: Kunden mit Apple-Handy werden angeblich bei Amazon höhere Preise angezeigt. Weiterhin sollen Amazon-Preise auch je nach Tageszeit variieren.[38]
- Sammlung und Weiterverkauf von Daten als Geschäftsmodell.
- Illegale Absichten: Erpressung, Spionage (auch Wirtschaftsspionage)

d) Ist das erlaubt?

- Es gibt in Deutschland Datenschutzgesetze, die besagen, dass die Menschen darüber informiert werden müssen, wie ihre Daten weiterverwendet werden. Aber:
  - Viele Firmen sitzen nicht in Deutschland und unterliegen nicht unseren Gesetzen.
  - Daten werden durch mehrere Länder transportiert, ehe sie am Ziel ankommen.
  - Auch deutsche Firmen halten sich nicht immer an die Gesetze.
  - Viele Menschen akzeptieren Datenbestimmungen, ohne sie gelesen zu haben.
- Interessant ist die Diskussion folgender Analogie: *Warum schließt du dein Fahrrad ab? Klauen ist doch verboten!*

e) Veranschaulichen von Tracking:

- **Wege von Datenströmen** im Netz werden veranschaulicht mit der *traceroute* von *dnstools*[39]*.* (Das Tool liefert noch mehr: z.B. die eigene IP-Adresse)

38 *http://www.chip.de/news/Fieser-Preistrick-bei-Amazon-Zahlen-Apple-Nutzer-wirklich-mehr_107203775.html* (Abgerufen am 6.5.18)
39 *dnstools.ch/visual-traceroute.html* (Abgerufen am 6.5.18)

- Die **eigene** aktuelle **IP-Adresse** und den ungefähren **Standort** findet man mit *utrace*[40].
- Mit der **IP**-Adresse kann man bei Maxmind[41] den zugehörigen **Namen** und Adresse heraus finden (und gleich kaufen).
- Veranschaulichung von Tracking direkt im Firefox-Browser: **lightbeam**[42] (firefox-Plugin)
- Mit track-your-tracker[43] kann man die **Tracker** einer Seite **anzeigen** lassen und findet viele weitere Informationen auf diesen Seiten.
- Bei *haveibeenpwned*[44] kann man prüfen, ob eine **E-Mail-Adresse** (nebst Passwort) z.B. im Rahmen eines Server-Angriffs **gestohlen** und/oder weiterverkauft wurde.
- Im **Video**: *Wenn die Verkäuferin eine App wäre* wird eine Analogie zwischen Bäckerei und einer App hergestellt und damit das App-Verhalten veranschaulicht: „Nennen Sie mir Ihre Telefonnummer!“ „Wo gehen Sie als nächstes hin?“,...)[45]
- Im **Video**: *Nackt im Netz*[46] *wird in einem interessanten Experiment gezeigt, welche teilweise kompromittierenden Informationen allein in URLs stecken.*

40 *https://www.utrace.de* (Abgerufen am 6.5.18)
41 *https://www.maxmind.com/en/geoip2-precision-demo* (Abgerufen am 6.5.18)
42 *z.B. bei: http://www.chip.de/downloads/Firefox-Lightbeam_65106174.html* (Abgerufen am 8.5.18)
43 *https://www.sit.fraunhofer.de/de/track-your-tracker/* (Abgerufen am 15.4.18)
44 *www.haveibeenpwned.com* (Abgerufen am 8.5.18)
45 *https://www.youtube.com/watch?v=wHo755bxByI* (Abgerufen am 15.4.18)
46 *https://www.youtube.com/watch?v=yGXb-ChrSFA* (Abgerufen am 15.4.18)