Informatik–Biber

Lehrmittel für die informatische Bildung an der Sekundarstufe I

Kommentar für Lehrpersonen

Inhaltsverzeichnis

Geheime Botschaften. Verschlüsseln – damit geheime Daten geheim bleiben

Ausgangskompetenz:

- Schülerinnen und Schüler können interaktive Webanwendungen nutzen.
- Schülerinnen und Schüler können Probleme analysieren und verschiedene Lösungsstrategien erproben.
- Schülerinnen und Schüler besitzen persönliche Passworte und halten diese geheim.
- Schülerinnen und Schüler können Informationen systematisch aus dem Internet beschaffen und deren Qualität abschätzen.
- Schülerinnen und Schüler kennen erste Verschlüsselungsverfahren, welche auf Substitution beruhen (Austausch einzelner Buchstaben).

Umsetzungsvorschläge (bis 4 Lektionen)

Lernenden-Perspektiven	Anschauen des Lernfilms Verschlüsseln – damit geheime Daten geheim bleiben Terminologie Kryptografie Einsatz von Verschlüsselung	
Arbeitsblatt 1	Botschaften verschlüsseln Bezug Lernfilm: E-Mail-Verschlüsselung (03:17)	
Arbeitsblatt 2	Schlüssel erraten / Geheimcode knacken Bezug Lernfilm: Schlüssellänge (04:09)	
Arbeitsblatt 3	Botschaften sicher verschlüsseln Bezug Lernfilm: Aktuelle Chiffrierverfahren (05:04)	
Biberaufgaben	Verschiedene Aufgaben zum Thema Verschlüsselung selbstständig lösen	
Mögliche Vertiefung	Interaktive Verschlüsselung *http://mgje.github.io/Crypto/* Unterrichtsmaterial für den Informatikunterricht *http://www.swisseduc.ch/informatik/* *http://www.educ.ethz.ch/unt/um/inf*	

Bildungsrelevanz des Themas gemäss Lehrplan 21 (aktuell diskutierte Vorarbeiten)

Nationale Grundkompetenzen für Themen der Informatik fehlen.

Kompetenzbereiche des Fachbereichs „Mathematik“

Die Schülerinnen und Schüler lernen Erforschen und Argumentieren. Sie können sich auf unbekannte Zahlenräume und Muster einlassen, Beispiele zu Gesetzmässigkeiten suchen, die erlangten Ergebnisse beschreiben, überprüfen, hinterfragen, interpretieren und begründen.

Kompetenzbereiche des Fachbereichs „Natur, Mensch, Gesellschaft“

- Die Schülerinnen und Schüler können selbst gemessene Grössen in einfachen Diagrammen darstellen und miteinander in Beziehung setzen.
- Die Schülerinnen und Schüler können Besonderheiten, Unterschiede und Zusammenhänge verschiedener Signale beobachten, beschreiben und erklären.
- Die Schülerinnen und Schüler können zu ausgewählten Erfindungen Informationen erschliessen und die Funktionsweise, angeleitet mit einfachen Experimenten, untersuchen.
- Die Schülerinnen und Schüler können technische Erfindungen untersuchen, die Entwicklung einer Erfindung schrittweise nachvollziehen und über die Folgen für den Alltag nachdenken.

Hintergrundwissen zur Verschlüsselung

Jegliche Kommunikation kann prinzipiell abgehört werden. Das heisst, wenn eine Textmitteilung per SMS oder Nachrichten-App versendet wird, kann diese durch Unbefugte gelesen werden. Falls Informationen so versendet werden sollen, dass nur die empfangende Person diese nutzen kann, sollten diese sicher verschlüsselt werden.
In diesem Modul werden Grundlagen der Verschlüsselung, der Kryptografie, an einfachen Verfahren besprochen. Im Abschnitt „Mögliche Vertiefungen“ wird der Einsatz von sicheren, jedoch komplexeren Verschlüsselungsverfahren besprochen.

Eine Herausforderung bei der Verschlüsselung einer Nachricht besteht darin, dass alle Menschen ausser der empfangenden Person nichts mit der verschlüsselten Nachricht anfangen können. Als Metapher wird häufig ein Schloss verwendet, welches die Botschaft in einem Couvert schützt. Nur die empfangende Person hat einen Schlüssel, mit welchem sie die Informationen entschlüsseln und dann lesen kann.

Klassische Verschlüsselungsverfahren sind so aufgebaut, dass Sender und Empfänger einen gemeinsamen geheimen Schlüssel besitzen. Der Sender verwendet diesen Schlüssel, um eine Botschaft zu verschlüsseln, der Empfänger verwendet das gleiche Geheimnis (Schlüssel), um die Botschaft zu entschlüsseln. Solche Verfahren nennt man symmetrisch. In diesem Modul werden einfache symmetrische Verschlüsselungsverfahren betrachtet. Diese ersetzen ein- und denselben Buchstaben durch immer ein- und dasselbe Symbol. Zum Beispiel könnte der Klartextbuchstabe E stets mit dem Geheimtextbuchstaben b chiffriert werden.

Terminologie

Die Begriffe *Kryptologie* und *Kryptografie* sind aus den griechischen Wörtern kryptos (geheim), logos (das Wort, der Sinn, der Gedanke) und *gráphein* (schreiben) gebildet. Beide Worte beziehen sich auf die Kunst, die sich mit Methoden zur Verheimlichung von Nachrichten beschäftigt. Die *Kryptoanalyse* ist die Wissenschaft, Kryptosysteme zu brechen und dann geheime Botschaften zu entschlüsseln.

Der Text, die Nachricht, die Buchstaben- oder Zeichenfolge, die wir übermitteln wollen, heisst der *Klartext*; in den folgenden Beispielen wird der Klartext in der Regel durch grosse Buchstaben (A,B,C, ...) repräsentiert. Eine verschlüsselte Nachricht (also eine Zeichenfolge, welche übermittelt werden soll), nennen wir den Geheimtext; diesen werden wir in Kleinbuchstaben (a,b,c, ...) schreiben. Der Verschlüsselungsvorgang wird als *chiffrieren* bezeichnet, der Entschlüsselungsvorgang als *dechiffrieren*. Kurz: **Ein Sender chiffriert einen Klartext und ein Empfänger dechiffriert einen Geheimtext.**

Die Texte, welche verschlüsselt werden, bestehen aus *Zeichen*, die Zeichen bilden insgesamt ein *Alphabet*. In den Beispielen zu diesem Modul wird das natürliche Alphabet {a, b, c, ..., x, y, z} verwendet. Die Sonderzeichen werden in den Beispielen nicht chiffriert und direkt übernommen. Umlaute können in der Form *ae*, *oe* und *ue* chiffriert werden.

Verschiebechiffren

Es existieren Briefe an Julius Cäsar (100 bis 44 v. Chr.), in welchen eine Geheimschrift verwendet wurde, welche die Buchstaben in veränderter Ordnung verwendete. Die von Cäsar verwendete Verschlüsselung erhält man, wenn man unter ein Klartextalphabet ein Geheimtextalphabet schreibt und es um drei Stellen nach links versetzt.

A	B	C	D	E	F	G	H	I	J
d	e	f	g	h	i	j	k	l	m
K	L	M	N	O	P	Q	R	S	T
n	o	p	q	r	s	t	u	v	w
U	V	W	X	Y	Z				
x	y	z	a	b	c				

Ein Klartext-Wort wie z.B. ‚ITALIEN' wird mithilfe der Cäsar-Chiffrierung als

lwdolhq

übertragen.

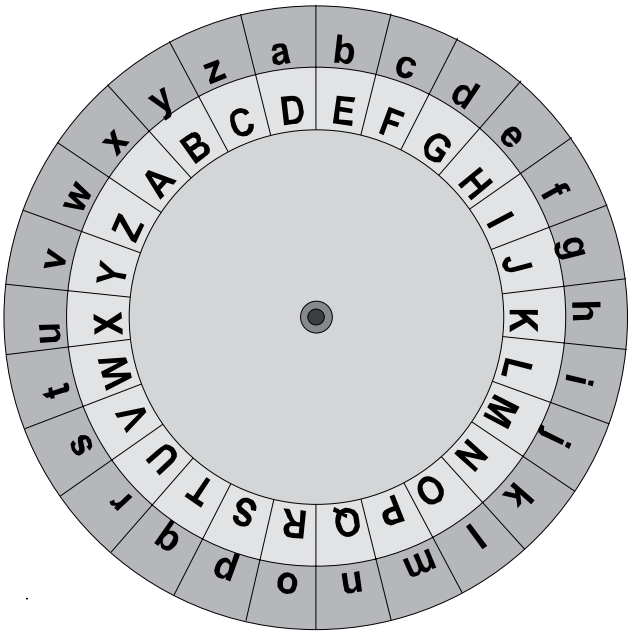
Auf die Frage, warum bei der *Cäsar-Chiffrierung* die Buchstaben gerade um drei Stellen nach links verschoben werden, gibt es keine Antwort. Eine weitere Verschiebechiffre ist die *Rot-13-Chiffrierung*. Sie verschiebt die Buchstaben um 13 Zeichen nach links, respektive um 13 Zeichen nach rechts. Bei einem Alphabet, bestehend aus 26 Buchstaben, ist diese Chiffrierung symmetrisch bezüglich der chiffrierten Zeichen.
Ein Klartext-Zeichen ‚A' wird zu einem Geheimtext-Zeichen ‚n' und ein ‚N' zu einem ‚a'. Das Klartext-Wort ‚CHIFFRIERUNG' wird bei der Rot-13-Chiffrierung zu

puvssevrehat

Verwendet man ein Alphabet, bestehend aus 26 Zeichen, gibt es 25 mögliche Verschiebechiffren, was in der folgenden Tabelle dargestellt ist.

Klartextalphabet:	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
Geheimtextalphabet.:	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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
	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

Mithilfe einer Chiffriermaschine lassen sich alle 25 Verschiebechiffren erzeugen.



Kryptoanalyse

Damit eine Verschlüsselung als möglichst sicher gelten kann, sollte diese mit allen möglichen Mitteln getestet werden. Aus diesem Grund ist das Knacken von Verschlüsselungen, die Kryptoanalyse, ein bedeutendes Teilgebiet der Kryptologie. Wechseln wir also die Rolle und spielen den Bösewicht. Wir stellen uns vor, dass Mr. X die Botschaft

crljreev uzv kiveuzxv jkruk rd xvewvijvv

abgefangen hat. Mit welcher Methode kann er diese Botschaft entschlüsseln?
Eine Möglichkeit, eine verschlüsselte Botschaft zu entschlüsseln, ist das systematische Durchprobieren. Mr. X kann vermuten, dass die Botschaft mit einer Verschiebechiffre verschlüsselt wurde. Er kann nun alle 25 Möglichkeiten mithilfe der Chiffriermaschine durchprobieren.
Als zweite Methode kann eine statistische Analyse durchgeführt werden. In einem Text kommen nicht alle Buchstaben gleich häufig vor. In der deutschen Sprache kommt der Buchstaben ‚e' am häufigsten (17,40 %) vor. Anhand der folgenden Tabelle kann nun eine Rangliste der häufigsten Buchstaben in der deutschen Sprache erstellt werden.

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6,51%	n	9,78%
b	1,89%	o	2,51%
c	3,06%	p	0,79%
d	5,08%	q	0,02%
e	17,40%	r	7,00%
f	1,66%	s	7,27%
g	3,01%	t	6,15%
h	4,76%	u	4,35%
I	7,55%	v	0,67%
j	0,27%	w	1,89%
k	1,21%	x	0,03%
l	3,44%	y	0.04%
m	2,53%	z	1,13%

Je nach Text variieren die Häufigkeiten der einzelnen Buchstaben. Eine Aufteilung der Buchstaben in vier Gruppen hilft bei der Entschlüsselung von Geheimbotschaften.

Gruppe	Gesamthäufigkeit dieser Buchstaben
e, n	27,18%
i, s, r, a, t	34,48%
d, h, u, l, c, g, m, o, b, w, f, k, z	36,52%
p, v, j, y, x, q	1,82%

Die Buchstaben der ersten beiden Gruppen (e,n,i,s,r,a,t) kommen über 3/5 (60%) in einem deutschen Text vor. Im Gegensatz dazu sind die Buchstaben p,v,j,y,x,q der vierten Gruppe sehr selten.
Bei der Chiffrierung eines deutschen Klartexts bleibt die Häufigkeitsverteilung erhalten, allerdings sind die Häufigkeiten neuen Buchstaben zugeordnet. Konkret geht Mr. X bei einer Kryptoanalyse wie folgt vor: Er zählt, wie häufig die einzelnen Buchstaben im Geheimtext enthalten sind.

Botschaft: crljreev uzv kiveuzxv jkruk rd xvewvijvv

Buchstabe: 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
Häufigkeit: 0 0 1 1 4 0 0 0 2 3 3 1 0 0 0 0 0 4 0 0 3 8 1 2 0 2

Klartextalphabet: 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
Geheimtextalphabet: 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

Der häufigste Buchstabe im Geheimtext ist v, Mr. X wird vermuten, dass v dem Buchstaben e entspricht. Falls diese Vermutung richtig ist, liegt eine Verschiebung um 17 resp. 9 vor. Eine Überprüfung ergibt, dass diese Vermutung richtig war.

Mit der entsprechenden Verschiebechiffre erhält man den Klartext „LAUSANNE DIE TRENDIGE STADT AM GENFERSEE“.

Algorithmus: Statistische Analyse von Verschiebechiffren
Man bestimmt den häufigsten Buchstaben im Geheimtext und verschiebt das Geheimtextalphabet so, dass dieser Buchstabe dem Klartext entspricht.

Monoalphabetische Chiffrierungen

Eine monoalphabetische Chiffrierung ordnet jeden Klartext-Buchstaben genau einem Geheimtext-Buchstaben zu. Neben den Verschiebechiffren gibt es eine grosse Zahl weiterer monoalphabetischer Chiffrierungen, wie zum Beispiel die folgende Chiffrierung:

Klartextalphabet: 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
Geheimtextalphabet: c v g i l p q y x z a w u b m o s h e k d j n r f t

Eine monoalphabetische Chiffrierung entspricht einer beliebigen Umordnung (Permutation) der Elemente des Klartext-Alphabets. Eine 26–elementige Menge hat genau 26! – 1 = 26 x 25 x ... x 2 x 1 – 1 = 403 291 461 126 605 635 583 999 999 ≈ $4 \cdot 10^{26}$ Permutationen. Diese ungeheuer grosse Anzahl an Verschlüsselungsmöglichkeiten täuscht eine Sicherheit vor. Im folgenden Abschnitt werden wir sehen, dass es Verfahren gibt, welche jede monoalphabetische Verschlüsselung knacken können.
Mr. X fängt wieder eine verschlüsselte Botschaft ab, dieses Mal mit ungefähr 500 Zeichen. Als Erstes zählt er die Häufigkeit der vorkommenden Buchstaben. Er kann die häufigsten vorkom-

menden Buchstaben der Gruppe e, n, i, s, r, a, t zuordnen. Jedoch eine Identifizierung der einzelnen Buchstaben gelingt in der Regel noch nicht vollständig. Als nächsten Schritt zählt Mr. X die Bigramme, damit bestimmt er die Häufigkeit aufeinanderfolgender Buchstaben und vergleicht diese mit der folgenden Tabelle.

Bigramm	Häufigkeit	Bigramm	Häufigkeit
en	3,88%	nd	1,99%
er	3,75%	ei	1,88%
ch	2,75%	ie	1,79%
te	2,26%	in	1,67%
de	2,00%	es	1,52%

Damit kann er weitere Buchstaben isolieren. Zum Beispiel hat das Paar „er“ eine sehr grosse Häufigkeit, während alle anderen Kombinationen der Buchstaben mit „e“ ziemlich selten vorkommen. („ea“ und „et“ sind wirklich sehr selten (unter 0,5%). Auch das Paar „es“ kommt mit signifikant geringerer Häufigkeit vor. Damit kann Mr. X die meisten der häufigsten Buchstaben identifizieren.
Am folgenden Beispiel wird ein mögliches Vorgehen an einem konkreten Beispiel schrittweise vorgestellt. Mr. X arbeitet mit einer interaktiven Kryptoanalyse. (Diese Webanwendung befindet sich im Download-Material oder kann direkt durch den folgenden Link http://mgje.github.io/Crypto benutzt werden.) Die geheime Botschaft wird durch Kleinbuchstaben dargestellt. Entschlüsselte Fragmente der Botschaft werden mit Grossbuchstaben angezeigt.

Nehmen wir an, das Mr. X die folgende Botschaft abfängt:

sdi lrdejgi fudysd ydmdu sjd gqydclqjchd vjdsduhduiodqqyeg idjedi irhedi vbu gudeadeqri. du hbdood sdw buaod gdue sbi adhefbchd sdu xduiturchdede mdqrheyeg gdabhqo sdu buao bmdu qdheod sjdid gebsd bm yes xduqbegod ldjede gurdiidude qrhe bqi dje ioydcl qbes je sdu gdgdes sdi udjchdi, vr idjed gdmyuoiiobso iobes, yes vr sdu gbood gdfbegde ibii, vdee jhe sdu ors ejcho mdfudjo hbood. sjd mjood vyusd ejcho eyu rhed vdjodudi aygdiobesde, iresdue sdu lrdejg mdfbhq bych, sjd gudeade sdi gdichdelode qbesioujchdi ir vdjo byiaysdhede, sbii mdjebhd sdu xjduod odjq sdi udjchdi be qbes yes qdyode sdi srcorui dumdjgdeoyw vyusd. ebch djejgde obgde vbu sjd ichdelyegiyulyesd gdujchoqjch byigdiodqqo yes wjo sdw lrdejgqjchde jeijdgdq mdlubdfojgo.

Achtung: Sonderzeichen wie Leerzeichen, Kommas usw. wurden nicht verschlüsselt. Umlaute ä, ö, ü wurden als ae, oe und ue geschrieben.

Eine statistische Analyse des Textes ergibt das Folgende:

Total Zeichen	737	
Chiff. Zeichen	617	
a	8	1.3%
b	33	5.3%
c	18	2.9%
d	122	19.8%
e	65	10.5%
f	6	1.0%
g	29	4.7%
h	29	4.7%
i	44	7.1%
j	38	6.2%
k	0	0.0%
l	10	1.6%
m	11	1.8%
n	0	0.0%
o	40	6.5%
p	0	0.0%
q	22	3.6%
r	17	2.8%
s	42	6.8%
t	1	0.2%
u	41	6.6%
v	10	1.6%
w	4	0.7%
x	3	0.5%
y	24	3.9%
z	0	0.0%

Die am häufigsten vorkommenden Buchstaben sind

d: 122 e: 65 i: 44 s: 42 u: 41 o: 40 j: 38
b: 33 g: 29 h: 29

Dank dieser statistischen Untersuchung lassen sich die ersten beiden Buchstabenpaare zuordnen:

d → E e → N

Die Buchstaben der zweiten Gruppe (I,S,R,A,T) können durch systematisches Ausprobieren den Buchstaben mit der folgenden Häufigkeit (i,s,u,o,j,b,g,h) zugeordnet werden.

j → I i → S u → R b → A o → T

Aus dieser ersten Zuordnungsrunde ergibt sich das folgende dechiffrierte Textfragment:

> sES lrENIgS fREysE yEmER sIE gqyEclqIchE vIEsERhERSTEqqyNg SEINES SrhNES vAR gRE-NaENqrS. ER hAETTE sEw ARaTE gERN sAS aEhNfAchE sER xERStRrchENEN mEqrhNyNg gE-aAhqT sER ARaT AmER qEhNTE sIESE gNAsE Am yNs xERqANgTE lEINEN gRrESSEREN qrhN AqS EIN STyEcl qANs IN sER gEgENs sES REIchES, vr SEINE gEmyRTSSTAsT STANs, yNs vr sER gATTE gEfANgEN SASS, vENN IhN sER Trs NIchT mEfREIT hATTE. sIE mITTE vyRsE NIchT NyR rhNE vEITERES aygESTANsEN, SrNsERN sER lrENIg mEfAhq Aych, sIE gRENaEN sES gESchEN-lTEN qANsSTRIchES Sr vEIT AySaysEhNEN, sASS mEINAhE sER xIERTE TEIq sES REIchES AN qANs yNs qEyTEN sES srcTrRS ERmEIgENTyw vyRsE. NAch EINIgEN TAgEN vAR sIE SchEN-lyNgSyRlyNsE gERIchTqIch AySgESTEqqT yNs wIT sEw lrENIgqIchEN INSIEgEq mElRAEfTIgT.

Die schwarzen Grossbuchstaben sind bereits entschlüsselt, die hellgrauen Kleinbuchstaben sind noch nicht dechiffriert.
Nun können verschiedene weitere Zuordnungen erprobt werden.

Zum Beispiel könnte der erste Buchstaben ein D sein (s → D), damit ergibt sich das Wort DES. Mit gNADE könnte GNADE gemeint sein, also g → G. Und mit hAETTE könnte HAETTE gemeint sein h →H. Auf ähnliche Weise finden sich die folgenden Zuordnungen:

c → C y → U l → K q → L r → O g → G f → F
s →D h → H m → B a → Z w → M x → V t → P
v → W

> DES KOENIGS FREUDE UEBER DIE GLUECKLICHE WIEDERHERSTELLUNG SEINES SOHNES WAR GRENZENLOS. ER HAETTE DEM ARZTE GERN DAS ZEHNFACHE DER VERSPROCHENEN BELOHNUNG GEZAHLT. DER ARZT ABER LEHNTE DIESE GNADE AB UND VERLANGTE KEINEN GROESSEREN LOHN ALS EIN STUECK LAND IN DER GEGEND DES REICHES, WO SEINE GEBURTSSTADT STAND, UND WO DER GATTE GEFANGEN SASS, WENN IHN DER TOD NICHT BEFREIT HATTE. DIE BITTE WURDE NICHT NUR OHNE WEITERES ZUGESTANDEN, SONDERN DER KOENIG BEFAHL AUCH, DIE GRENZEN DES GESCHENKTEN LANDSTRICHES SO WEIT AUSZUDEHNEN, DASS BEINAHE DER VIERTE TEIL DES REICHES AN LAND UND LEUTEN DES DOCTORS ERBEIGENTUM WURDE. NACH EINIGEN TAGEN WAR DIE SCHENKUNGSURKUNDE GERICHTLICH AUSGESTELLT UND MIT DEM KOENIGLICHEN INSIEGEL BEKRAEFTIGT.

Moderne monoalphabetische Algorithmen

Eine häufig verwendete monoalphabetische Chiffrierung ist der *Data Encryption Standard (DES)*. Dieser wurde im Wesentlichen von IBM entwickelt und 1977 standardisiert. Der DES verschlüsselt nicht Buchstaben, sondern die Symbole 0 und 1 und zwar jeweils 64 auf einmal. Der DES-Algorithmus wurde von Anfang an vollständig publiziert – es war der erste Verschlüsselungs-

Algorithmus der Geschichte, bei dem das der Fall war.
Wegen zu kurzer Schlüssellängen kann eine DES-Chiffrierung mit heutigen Computer innerhalb von Minuten geknackt werden. Aus diesem Grund wurde bereits im Herbst 2000 ein neuer Standard für symmetrische Verschlüsselung vorgeschlagen. Die Chiffriermethode für den *Advanced Encryption Standard (AES)* wurde durch eine öffentliche Ausschreibung gefunden. Gewonnen hat ein europäisches Team um Joan Daemen und Vincent Rijmen.

Bis heute ist keine Methode bekannt, welche eine mit AES chiffrierte Botschaft und gut gewähltem Passwort knacken kann. Es ist wichtig zu betonnen, dass die Sicherheit direkt von der Wahl des Passworts abhängt. Passwörter, welche zu kurz sind, eine lexikale Bedeutung besitzen oder keine Sonderzeichen beinhalten, können mithilfe von Computern durch systematisches Durchprobieren erraten werden.

Weitere Informationen zu guten Passwörtern findet man auf den folgenden Seiten:
- https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html
- http://www.sicherespasswort.com/
- http://www.wiesicheristmeinpasswort.de/

Monoalphabetische Chiffrierung natürlicher Sprachen ist unsicher
Weil die Häufigkeit der vorkommenden Buchstaben in natürlichen Sprachen bekannt ist, können durch verschiedene Verfahren geheime Botschaften entschlüsselt werden, welche auf dem natürlichen Alphabet basieren. Heutzutage werden deshalb monoalphabetische Chiffrierungen über binär kodierte Blöcke verwendet. Diese werden in mehreren Durchläufen mit verschiedenen Schlüsseln chiffriert. Eine häufig verwendete Verschlüsselung ist momentan der *Advanced Encryption Standard (AES)*.

Anmerkung zur Sicherheit im Internet
In diesem Modul wurde aufgezeigt, dass es viele Chiffriermethoden (Algorithmen) gibt, welche leicht zu entschlüsseln sind. Die Wahl einer modernen sicheren Chiffriermethode genügt jedoch noch nicht, um sicher vor Informationsdiebstal zu sein. Die Sicherheit eines Systems hängt stark davon ab, wie die Handhabung der Schlüssel (Keystore), wie aktuell die Verschlüsselungssoftware (Updates) und wie unversehrt das verwendete System (Viren) ist. Das sind leider viele Gründe, seinem Smartphone oder Computer prinzipiell nicht zu trauen.

Umsetzungshilfen

Reflexion Lernfilm / Perspektiven der Lernenden

Im Plenum wird der Lernfilm „Verschlüsseln – damit geheime Daten geheim bleiben“ geschaut.

Zur Reflexion des Lernfilms können folgende Fragen in der Klasse aufgenommen werden:

- Welche Möglichkeiten kennt ihr, um Botschaften auszutauschen?
- Was bedeutet sicher kommunizieren?
- Können E–Mails durch Dritte gelesen werden?
- Welche Schülerinnen verschlüsseln ihre Text-Nachrichten (Botschaften) bereits heute?

Arbeitsblatt 1: „Botschaften verschlüsseln“

Die Schülerinnen und Schüler lernen verschiedene monoalphabetische Verschlüsselungsmethoden. Durch die Anwendung verschiedener Verfahren entdecken sie, dass bei diesen Verfahren der gleiche Schlüssel für die Verschlüsselung wie auch die Entschlüsselung verwendet wird. Deshalb wird diese Verschlüsselungstechnik als symmetrische Verschlüsselung bezeichnet. Im Weiteren sollen die Schülerinnen und Schüler herausfinden, dass es 25 unterschiedliche Verschiebechiffren, aber 403 291 461 126 605 635 583 999 999 $\approx 4 \cdot 10^{26}$ Möglichkeiten gibt Buchstaben monoalphabetisch zu vertauschen.

Arbeitsblatt 2: „Schlüssel erraten / Geheimcode knacken“

Die Schülerinnen und Schüler entschlüsseln verschiedene Botschaften. Sie lernen dabei, dass die monoalphabetischen Verfahren, welche Buchstaben auf andere Buchstaben abbilden, unsicher sind. In Form eines Wettbewerbs können gegenseitig verschlüsselte Botschaften geknackt werden.

Arbeitsblatt 3: „Botschaften sicher verschlüsseln“

In einem internationalen und öffentlichen Wettbewerb wurde das AES-Verfahren im Jahr 2000 ausgewählt. Es gilt bis heute als sicher. Mithilfe einer Webanwendung können die Schülerinnen und Schüler ihre Textbotschaften sicher verschlüsseln.

Informatik-Biberaufgaben zum Thema „Geheime Botschaften“

Die Biberaufgaben stellen konkrete Fragen zu Themen im Umfeld der Verschlüsselung. Sie wurden den drei Schwierigkeitsstufen einfach, mittel, schwierig zugeordnet und liegen in den entsprechenden Verzeichnissen.

Weitere Informationen zum Informatik-Biber-Wettbewerb finden Sie auf der Webseite *http://www.informatik-biber.ch/*

Mögliche Vertiefungen

- Interaktive Verschlüsselung, *http://mgje.github.io/Crypto/*
- Historische Chiffrierverfahren, *http://www.cryptool-online.org/*
- Sicherheit, *http://www.swisseduc.ch/informatik/internet/internet_sicherheit/*
- DES, *http://www.matheprisma.de/Module/DES/index.htm*
- AES, *http://www.heise.de/developer/artikel/Cryptography-Engineering-Teil-1-Zur-Theorie-des-Advanced-Encryption-Standard-1350362.html*
- Cryptographic Protocols, *http://csunplugged.org/cryptographic-protocols*
- Public Key Encryption, *http://csunplugged.org/public-key-encryption*
- Asymmetrische Kryptographie für die Sek I, *http://bscw.schule.de/pub/bscw.cgi/d938724/RSA_fast_ohne_Mathematik.pdf*
- Crypto CD-ROM (Simon Singh, englisch) *http://simonsingh.net/cryptography/crypto-cd-rom/*
- Unterrichtsmaterialien Informatik, *http://www.educ.ethz.ch/unt/um/inf*

Weiterführende Literatur

Hromkovic, J. (2006). *Sieben Wunder der Informatik.* Wiesbaden: Vieweg + Teubner Verlag.

Freiermuth, K., Hromkovic, J., Keller, L., & Steffen, B. (2010). *Einführung in die Kryptologie: Lehrbuch für Unterricht und Selbststudium.* Springer DE.

Borys, T. (2011). *Codierung und Kryptologie.* ISBN 978-3-8348-1706-8, Wiesbaden: Vieweg + Teubner Verlag.

Dankmeier, W. (2006). *Grundkurs Codierung: Verschlüsselung, Kompression, Fehlerbeseitigung.* ISBN 978-3-8348-9009-2, Wiesbaden: Vieweg + Teubner Verlag.

Beutelspacher, A. (2007). *Kryptologie.* ISBN 978-3-8348-0253-8, Wiesbaden: Vieweg & Sohn Verlag.

Buchmann, J. (2009). *Einführung in die Kryptographie.* ISBN 978-3-642-11185-3, Springer DE.

DES, Kapitel 6 in Buchmann, J. (2009).

Lösungen

Aufgabenblatt 1: „Botschaften verschlüsseln“

Arbeitsauftrag 2, z.B. Klartext: „DAS IST EIN GEHEIMNIS“, Schlüssel: um 4 Positionen verschieben, Geheimtext: „yvn dno zdi bzczdhidn“.

Arbeitsauftrag 3: Zuordnungstabelle

Klartextalphabet: 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
Geheimtextalphabet: c v g i l p q y x z a w u b m o s h e k d j n r f t
Der Klartext „DAS IST EIN GEHEIMER TEXT“ wird zum Geheimtext „ice xek lxb qlylxulh klrk“.

Arbeitsauftrag 4: Zuordnungstabelle

Klartextalphabet: 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
Geheimtextalphabet: i d c p y l r g j v o f t b z x w n a u k q e h s m
Der Klartext „BERN IST DIE HAUPTSTADT“ wird zum Geheimtext „dynb jau pjy gikxuauipu“.
Der Geheimtext kann mit analytischen Verfahren entschlüsselt werden, siehe Aufgabenblatt 2.

Antworten zu den Fragen:

1. Es gibt 25 Verschiebeverschlüsselungen.
2. Die maximale Anzahl der monoalphabetischen Verschlüsselungen entspricht der Anzahl aller Permutationen der vorkommenden Buchstaben minus 1.
3. Also $26!-1 = 403\,291\,461\,126\,605\,635\,583\,999\,999 \approx 4 \cdot 10^{26}$
4. Bei der monoalphabetischen Verschlüsselung wird jedem Klartextbuchstaben genau ein Geheimtextbuchstaben zugeordnet.

Aufgabenblatt 2: „Schlüssel erraten / Geheimcode knacken“

Antworten zu den Fragen:

1. Der Geheimtext „dooh zhjh ixhkuhq qdfk urp“ kann durch eine Verschiebung aller Buchstaben um 3 Positionen als Klartext „ALLE WEGE FUEHREN NACH ROM“ entschlüsselt werden.
2. Der Geheimtext „va jvexyvpuxrvg tvog rf ahe qvr ngbzr haq qnf yrrer“ kann als folgender Klartext „IN WIRKLICHKEIT GIBT ES NUR DIE ATOME UND DAS LEERE“ entschlüsselt werden (Zitat von Demokrit, griechischer Naturphilosoph).
3. Der Geheimtext „jivsompmquvqa“ kann mit einer Verschiebechiffre (acht Positionen) zum Klartext „BANKGEHEIMNIS“ dechiffriert werden.
4. Der Geheimtext „mrnbna cngc rbc wrlqc vnqa pnqnrv“ kann zum Klartext „DIESER TEXT IST NICHT MEHR GEHEIM“ entschlüsselt werden.

   Da es nur 25 Möglichkeiten gibt, kann die Verschiebeverschlüsselung rasch durch Ausprobieren geknackt werden. Das geht z.B. mit der Cäsar-Scheibe oder der interaktiven Entschlüsselung *http://mgje.github.io/Crypto/exp3/* .

5. Der Geheimtext
„wix jgrix nghzri udr rglrihwih aähwih eb lidhiu lilliy bhw ydill ldta adhidhqgyyih; il lga gbl, gyl lrxitzi ix ldta eb lidhiu pinöahydtaih gvihwltayäqtaih, gvix wgl lrgxzi hdtzih lidhil ndi agyryolih zofqil eidpri, wgll ix pghe bhw pgx hdtar ltaydiq. pxipox ngx wdi pghei eidr lrdyy gbq wiu fygre piyipih, gbq wiu dah wdi eduuixaixxih ixrgffr agrrih. wdi ihrräbltabhp üvix wgl udllydhpih lidhil fyghil, jdiyyidtar gvix gbta wdi wbxta wgl jdiyi abhpixh jixbxlgtari ltanätai ugtarih il dau bhuöpydta, ldta eb vinipih. ix qüxtariri udr idhix pindllih vilrduuraidr ltaoh qüx wih hätalrih gbpihvydtz idhih gyypiuidhih üvix dah ldta ihrygwihwih eblguuihlrbxe bhw ngxriri. hdtar idhugy wdi jdoydhi ltaxitzri dah gbq, wdi, bhrix wih edrrixhwih qdhpixh wix ubrrix aixjox, dax jou ltaolli qdiy bhw idhih agyyihwih roh joh ldta pgv“

hat die folgende Häufigkeitstabelle der vorkommenden Buchstaben:

Geheimtextalph.:	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
Häufigkeit:	41	23	0	55	12	5	38	72	116	8	0	51	0	8	10	19	11	41	0	29	20	9	28	37	29	7

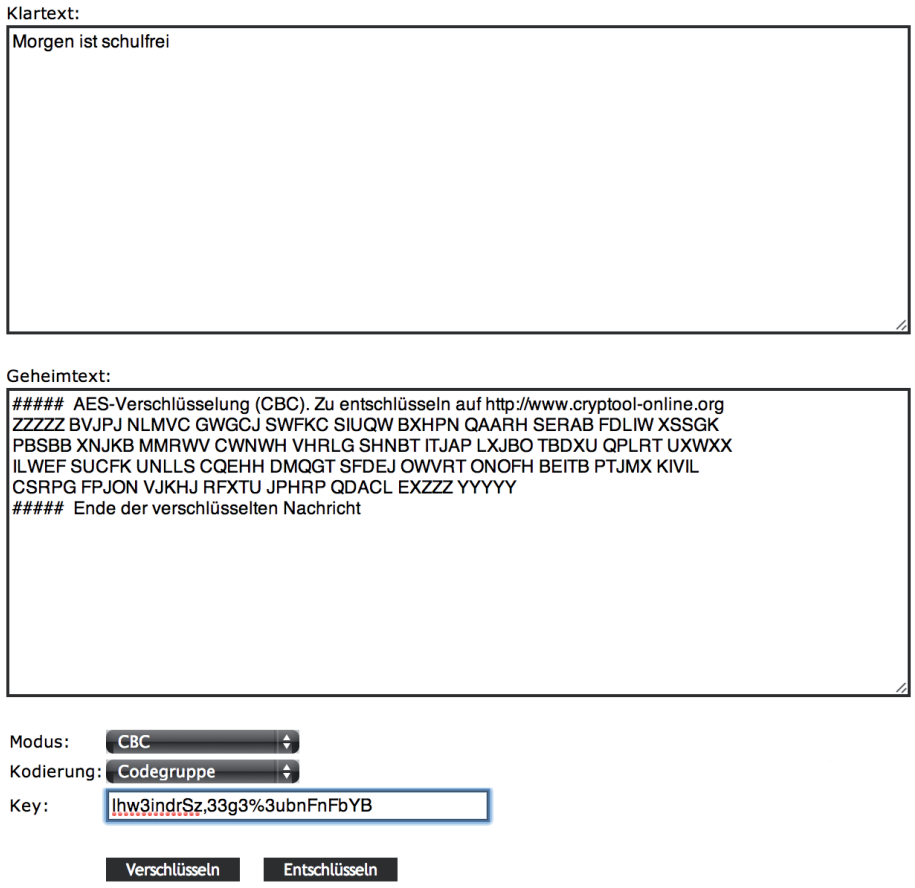
Mit der folgenden Zuordnungstabelle ...

Geheimtextalphabet:	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
Klartextalphabet:	H	U	-	I	Z	P	A	N	E	V	-	S	-	W	O	G	F	T	-	C	M	B	D	R	L	K

... erhält man den folgenden Klartext:
„DER VATER WANKTE MIT TASTENDEN HÄNDEN ZU SEINEM SESSEL UND LIESS SICH HINEINFALLEN; ES SAH AUS, ALS STRECKE ER SICH ZU SEINEM GEWÖHNLICHEN ABENDSCHLÄFCHEN, ABER DAS STARKE NICKEN SEINES WIE HALTLOSEN KOPFES ZEIGTE, DASS ER GANZ UND GAR NICHT SCHLIEF. GREGOR WAR DIE GANZE ZEIT STILL AUF DEM PLATZ GELEGEN, AUF DEM IHN DIE ZIMMERHERREN ERTAPPT HATTEN. DIE ENTTÄUSCHUNG ÜBER DAS MISSLINGEN SEINES PLANES, VIELLEICHT ABER AUCH DIE DURCH DAS VIELE HUNGERN VERURSACHTE SCHWÄCHE MACHTEN ES IHM UNMÖGLICH, SICH ZU BEWEGEN. ER FÜRCHTETE MIT EINER GEWISSEN BESTIMMTHEIT SCHON FÜR DEN NÄCHSTEN AUGENBLICK EINEN ALLGEMEINEN ÜBER IHN SICH ENTLADENDEN ZUSAMMENSTURZ UND WARTETE. NICHT EINMAL DIE VIOLINE SCHRECKTE IHN AUF, DIE, UNTER DEN ZITTERNDEN FINGERN DER MUTTER HERVOR, IHR VOM SCHOSSE FIEL UND EINEN HALLENDEN TON VON SICH GAB“

Aufgabenblatt 3: „Botschaften sicher verschlüsseln“

Mit der Webanwendung *http://www.cryptool-online.org/index.php?Itemid=135* können eigene Text sicher mit dem AES-Verfahren verschlüsselt werden.



Antworten zu den Fragen:

1. Wer hat die AES-Verschlüsselung erfunden?
   Die Chiffriermethode für den Advanced Encryption Standard (AES) wurde durch eine öffentliche Ausschreibung gefunden. Gewonnen hat ein europäisches Team um Joan Daemen und Vincent Rijmen.
2. Kann jemand eine mit AES chiffrierte Botschaft ohne Schlüssel lesen?
   Bis heute (Frühling 2014) ist keine Methode bekannt, welche eine AES-Botschaft mit einem langen Schlüssel in nützlicher Zeit entschlüsseln kann.
3. Worin besteht das Problem, wenn man jemandem eine AES-Botschaft zukommen lassen will?
   Das Problem liegt beim Austausch des Schlüssels! Dieser muss auf eine sichere Weise zum Empfänger transportiert werden. Eine Lösung dieses Problems bieten asymmetrische Verschlüsselungsverfahren. Bei diesen ist der Schlüssel zur Chiffrierung allen bekannt (öffentlich), der Schlüssel zur Dechiffrierung jedoch ist privat (geheim).

Impressum

Herausgeber	SVIA, Schweizerischer Verein für Informatik in der Ausbildung
Partner	Hasler Stiftung ICT Berufsbildung SWITCH
Konzeption / Umsetzung	Lernetz AG
Autor	Martin Guggisberg, PH FHNW