

Informatik–Biber

*Lehrmittel für die informatische
Bildung an der Sekundarstufe I*

Kopiervorlagen



Arbeitsblatt 01: Botschaften verschlüsseln

Fragestellung

Wie können Botschaften geheim übermittelt werden?

Benötigte Materialien

- Schere
- Kopiervorlagen

Zusätzliche Materialien

- Interaktive Verschlüsselung, <http://mgje.github.io/Crypto/>
- Historische Chiffrierverfahren, <http://www.cryptool-online.org/>

Arbeitsaufträge

1. Bastle eine Cäsar-Scheibe und verschlüsse deinen Namen mit der Verschiebechiffre 13.
2. Verschlüsse einen Satz, und übermittle diese verschlüsselte Botschaft deiner Nachbarin oder deinem Nachbarn.
3. Erstell eine eigene Zuordnungstabelle, welche 26 Klartextbuchstaben (Grossbuchstaben) 26 Geheimbuchstaben (Kleinbuchstaben) zuordnet.

Verschlüsse die Botschaft: **DAS IST EIN GEHEIMER TEXT**

Tipp: eine Zuordnungstabelle könnte wie folgt aussehen:

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

4. Wie kann eine geheime Botschaft entschlüsselt werden? Erstell eine Geheimbotschaft und dazu eine Entschlüsselungstabelle. Übermittle nun einer Nachbarin oder einem Nachbarn die geheime Botschaft mit der Entschlüsselungstabelle. Kann deine Botschaft gelesen werden?

Fragen

1. Wie viele verschiedene Verschiebeverschlüsselungen gibt es? (Bei einem Alphabet von 26 Zeichen)
2. Wie viele verschiedene monoalphabetische Verschlüsselungen können maximal erstellt werden?
3. Was bedeutet „monoalphabetisch verschlüsseln“?

Das Verschlüsseln mit Bleistift und Papier ist aufwendig. Falls eure Schule die Möglichkeit besitzt, das Internet zu benutzen, könnt ihr mithilfe der folgenden Webanwendung eigene Texte monoalphabetisch verschlüsseln.

Krypto

1 Cäsar
2 ROT-13
3 ROT-X
4 Monoalphabetisch
5 Entschlüsseln
6 Kryptoanalyse
7 **Knacknuss**

Info Geheimmisss

Neue

Knacknuss

Relativ

Absolut

1045

a	b	c	d	e	f	g	h	i	j
5.7%	4.4%	2.9%	6.4%	2.4%	0.0%	2.1%	1.9%	0.0%	0.4%

k	l	m	n	o	p	q	r	s	t
2.7%	5.5%	5.2%	6.3%	3.9%	1.2%	0.0%	11.2%	0.2%	4.6%

u	v	w	x	y	z				
2.2%	7.7%	3.2%	1.5%	0.2%	18.3%				

z	r	v	d	n	a	l	m	t	b
18.3%	11.2%	7.7%	6.4%	6.3%	5.7%	5.5%	5.2%	4.6%	4.4%

E	N	I	S	R	A	T	D	H	U
17,40%	9,78%	7,55%	7,27%	7,00%	6,51%	6,15%	5,08%	4,76%	4,35%

Entschlüsseln

dzv ar dzv wrnbrz tncf metxnet ord uwzaet bzxgvdzrz hnocknrr tnliz metgr bvnozm tnnv uzhgkkzr ord zarzr wrnbrz unvl, dzv atk uam pov tñwuzr uvomf vzaetfz. tãrdz ord cümmz xñvzr bzcmmzwl ord zar pzvczplzm bzxñrd uzdehlz mzarzr wzau. dzv tzvv bvnc lvnl mlgwpzr metvallzm ar dñr bzvaetlmñnnw; cüv atr, dñr vzaetzr, tgetbzugvzrzr knñr, bñu zm xgtw hzarzr bvord pov covetf. dzv rzoz bvordtzvv uzcntw mgbwzaet, dzk uam dñtar bzcnbrzr bztñwlzrzr hnocknrrz daz cmmzwr nuporztñzr ord maz dzk bvñczr nrpowbzr. guxgtw daz bzvaetlmtzvzr zarñrdzv jvzxordzvl nrñmtzr, xñblz dget hzarzr zar xgvl bzbzr daz nrgvdorrb dzm bzuaazlrdzr bvordtzvvr jgvpouvarbzr. szlpl cvñblz daz ar kãrrzvhwzadorb dñmltztzrdz cvno dñr bvñczr: »uzhzrrzl, xaz aml dñknwm daz bgwdzrz hlzlf dzv hnocknrrmcvno ar zovz tãrdz bzhgkkzr?« dzv bvñc zvxadzvlz kal metnkgwmzv cvzettzal: »daz cvno

Wie können Botschaften geheim übermittelt werden?

Eine Botschaft kann verschlüsselt werden. Damit macht man es einem Angreifer schwierig, die Botschaft zu lesen. Für viele Verschlüsselungsverfahren gibt es Techniken, die eine Entschlüsselung ermöglichen. Die hohe Rechenleistung aktueller Computer erlaubt es, dass Millionen von Passwörtern in Sekundenbruchteilen automatisch ausprobiert werden können. Aus diesem Grund ist neben der Wahl eines sicheren Verfahrens auch die Wahl eines sicheren Passworts zentral.

Viele verschiedene, jedoch auch unsichere Verschlüsselungsverfahren kannst du auf der folgenden Webseite ausprobieren: <http://www.cryptool-online.org/>

Arbeitsblatt 02: Geheime Botschaft knacken

Fragestellung

Wie kann eine geheime Botschaft ohne den nötigen Schlüssel trotzdem entschlüsselt werden?

Benötigte Materialien

- Cäsar-Scheibe (Arbeitsblatt 1)
- Schere
- Kopiervorlagen

Zusätzliche Materialien

- Interaktive Verschlüsselung, <http://mgje.github.io/Crypto/>
- Historische Chiffrierverfahren, <http://www.cryptool-online.org/>

Finde Antworten zu den folgenden Fragen:

1. Entschlüssele folgenden Text, wenn du weißt, dass es sich um die Cäsar-Verschlüsselung handelt.

dooh zhjh ixhkuhq qdfk urp

2. Entschlüssele folgenden Text, wenn du weißt, dass die ROT-13-Verschiebechiffre verwendet wurde.

va jvexyvpuxrvq tvog rf ahe qvr ngbzs haq qnf yrre

3. Der Geheimtext *jivsompmquvqa* wurde mit der Verschiebungschiffre erzeugt. Ermittle den Schlüssel und den Klartext.
4. Entschlüssele folgenden Text *mrnbna cngc rbc wrlqc vnqa pnqnr*, wenn du weißt, dass eine Verschiebechiffrierung verwendet wurde.
5. Der folgende Text wurde monoalphabetisch verschlüsselt. Entschlüssele ihn!
Tipp: Zähle als Erstes das Vorkommen der einzelnen Buchstaben. Vergleiche deine erhaltene Verteilung mit einer Statistik der deutschen Sprache (Kopiervorlage).

wix jgrix nghzri udr rglrihwih aähwih eb lidhiu lilliy bhw ydill ldta adhidhqgyyih; il lga gbl, gyl lr-
xitzi ix ldta eb lidhiu pinöahydtaih gvihwltayäqtaih, gvix wgl lrgxzi hdtzih lidhil ndi agyryolih
zofqil eidpri, wgl ix pghe bhw pgx hdtar ltaydiq. pxipox ngx wdi pghei eidr lrdyy gbq wiu fyg-
re piyipih, gbq wiu dah wdi eduuixaixxih ixrgffr agrrih. wdi ihrräbltabhp üvix wgl udlydhiph lid-
hil fyghil, jdiyyidtar gvix gbta wdi wbxta wgl jdiyi abhpixh jixbxltari ltanätai ugtarih il dau bhuö-

pydta, ldta eb vinipih. ix qüxtariri udr idhix pindllih vilrduuraidr ltaoh qüx wih hätalrih gbpihvydtz idhix gyypuiidhix 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 id-hih agyyihwih roh joh ldta pgv

6. Weitere Geheimnisse (verschlüsselte Texte) befinden sich in den Kopiervorlagen oder können von <http://mgje.github.io/Crypto/geheimnisse/> bezogen werden.

So geht's auch

Mithilfe der elektronischen Beilage können beliebige Texte auf verschiedene Art und Weise verschlüsselt und entschlüsselt werden. Verschlüsse einen kurzen Text, und gib diesen als geheime Botschaft einer Schulkollegin oder einem Schulkollegen zum Entschlüsseln.

Krypto
1 Cäsar 2 ROT-13 3 ROT-X 4 Monoalphabetisch 5 Entschlüsseln 6 Kryptoanalyse 7 **Knacknuss** Info Geheimnisse

Neue Knacknuss
Relativ Absolut 1045

a	b	c	d	e	f	g	h	i	j
5.7%	4.4%	2.9%	6.4%	2.4%	0.0%	2.1%	1.9%	0.0%	0.4%

k	l	m	n	o	p	q	r	s	t
2.7%	5.5%	5.2%	6.3%	3.9%	1.2%	0.0%	11.2%	0.2%	4.6%

u	v	w	x	y	z				
2.2%	7.7%	3.2%	1.5%	0.2%	18.3%				

z	r	v	d	n	a	l	m	t	b
18.3%	11.2%	7.7%	6.4%	6.3%	5.7%	5.5%	5.2%	4.6%	4.4%

E	N	I	S	R	A	T	D	H	U
17,40%	9,78%	7,55%	7,27%	7,00%	6,51%	6,15%	5,08%	4,76%	4,35%

dzv ar dzv wnrbrz tnci metxnet ord uwzaet bxzgydrz hnocknrr tnliz metgr bvnozm tnnv uzhgkkzr ord zarzr wnrbrz unvl, dzv atk uam pov tnwuzr uvoml vzaetiz. tärdz ord cümzmz xnvzr bzcmmzwl ord zar pzvczplzm bznrd uzdehlz mzarzr wzau. dzv tzvv bvnc lvnl mlgwpzr metvallzm ar dzt bzvaetlmmnw; cüv atr, dzt vzaetiz, tgetbzugvzrzn knrr, bnu zm xgtw hzarzr bvord pov covetl. dzv rzo bvordtzvv uzcntw mgbwzaet, dzk uam dntar bznrbzr bztwlvzrzn hnocknrrz dz cmmzwr nuportkzr ord maz dzk bvnczr nropwzbr. guxgtw dz bzvaetlmtzvzr zarnrdz jvzxordzvl nrmntzr, xnbiz dget hzarzr zar xgvl bzbzr dz nrgvdrorb dzm bzuaizlrdrz bvordtzvvr jgvpouvarbzr. szlpl cvnblz dz ar kärzvhwzadorb dnmiltzrdz cvno dzt bvnczr: »uzhzrrzl, xaz aml dknwm dz bgwdzr hllz dzv hnocknrmcvno ar zovz tärdz bzhgkkzr?« dzv bvnc zvxadzvlz kal metnkwgmzv cvzettal: »dz cvno

dzv ar dzv wnrbrz tnci metxnet ord uwzaet bxzgydrz hnock nrr tnliz metgr bvnozm tnnv uzhgkkzr ord zarzr wnrbrz unv l, dzv atk uam pov tnwuzr uvoml vzaetiz. tärdz ord cümzmz xnvzr bzcmmzwl ord zar pzvczplzm bznrd uzdehlz mzarzr wzau. dzv tzvv bvnc lvnl mlgwpzr metvallzm ar dzt bzvaet lmmnw; cüv atr, dzt vzaetiz, tgetbzugvzrzn knrr, bnu zm xgtw hzarzr bvord pov covetl. dzv rzo bvordtzvv uzcntw m gbwzaet, dzk uam dntar bznrbzr bztwlvzrzn hnocknrrz dz cmmzwr nuportkzr ord maz dzk bvnczr nropwzbr. guxgtw d az bzvaetlmtzvzr zarnrdz jvzxordzvl nrmntzr, xnbiz dget hzarzr zar xgvl bzbzr dz nrgvdrorb dzm bzuaizlrdrz bvordtzvvr jgvpouvarbzr. szlpl cvnblz dz ar kärzvhwzadorb d nmltztzrdz cvno dzt bvnczr: »uzhzrrzl, xaz aml dknwm dz bgwdzr hllz dzv hnocknrmcvno ar zovz tärdz bzhgkkzr?« dzv bvnc zvxadzvlz kal metnkwgmzv cvzettal: »dz cvno me tzhiz kav dz hllz nwm wazuzmynrd.« -- dnvoc xovdz da z knbd ar hllzr bhwzbl ord ar'm jvziöy bzhgkkzr; maz mgw wlvz zvhw ävzr xaz zm maet kal dzv hllz izutnalz dz zvm

Entschlüsseln

Weitere Beispiele zum Entschlüsseln finden sich in der elektronischen Beilage oder auf dem Internet unter dem Link <http://mgje.github.io/Crypto/exp7/>.

Antwort zu der Einstiegsfrage

Wie kann eine geheime Botschaft ohne den nötigen Schlüssel trotzdem entschlüsselt werden?

Die Kryptoanalyse ist die Wissenschaft, Kryptosysteme zu brechen und dann geheime Botschaften zu entschlüsseln.

Werkzeuge für die Kryptoanalyse finden sich auf der folgenden Webseite:

<http://www.cryptool-online.org/>

Arbeitsblatt 03: Botschaften sicher verschlüsseln

Fragestellung

Kann eine Botschaft sicher verschlüsselt werden? Sodass nur die vorgesehene empfangende Person mit einem entsprechenden Schlüssel diese lesen kann?

Benötigte Materialien

- Zugang zum Internet
- Webbrowser

Hintergrundinformation

Der *Advanced Encryption Standard (AES)* ist im Gegensatz zu den bis jetzt vorgestellten Verschlüsselungsverfahren eine sichere Methode, Botschaften zu chiffrieren. In einem internationalen und öffentlichen Wettbewerb wurde das Verfahren im Jahr 2000 ausgewählt. Bis zum Frühjahr 2014 konnte niemand AES verschlüsselte Botschaften ohne entsprechenden Schlüssel entschlüsseln. Aus diesem Grund gilt das AES-Verfahren als sicher, unter der Bedingung, dass ein genügend langer Schlüssel gewählt wird (momentan genügen zehn Zeichen).

AES-Verschlüsselung einer Botschaft: Vorgehen

1. Besuche die Webseite <http://www.cryptool-online.org/index.php?Itemid=135>
2. Wähle einen sicheren Schlüssel bis zu 32 Zeichen.
Tipp: Ein sicherer Schlüssel kann zum Beispiel aus einem Satz generiert werden, indem immer der erste und der letzte Buchstaben verwendet wird. Zusätzliche Sicherheit bieten Sonderzeichen. So kann z.B. für den Buchstaben *i* eine *!* genommen werden, für ein *e* eine *3* oder für ein *k* das %-Zeichen.

Aus dem Text...

Ich wohne in der Schweiz, esse gerne Käse und bin Fan vom Fussballclub YB

... ergibt sich der folgende Schlüssel:

Ihw3indrSz,33g3%3udbnFnFbYB

3. Mit diesem Schlüssel kann ein Text, z.B.
Morgen ist schulfrei
verschlüsselt werden.

Klartext:

Morgen ist schulfrei

Geheimtext:

AES-Verschlüsselung (CBC). Zu entschlüsseln auf <http://www.cryptool-online.org>
ZZZZZ UMKOD JSXCB QEHHX SQHJU BGJRR FIHMX KCJSM BCKDB OSBSS CMKEK
QESTX KGMRE JTETX FLDFM VHPJW QUXCV NDNUX ILKMC BEALA XDRUM JMPHT
WUKBL OSUUP ONUHA IGVIF GOKZZ YYYYY
Ende der verschlüsselten Nachricht

Modus:

Kodierung:

Key:

Verschlüsseln

Entschlüsseln

4. Übermittle den Geheimtext deiner Nachbarin oder deinem Nachbarn, z.B.
AES-Verschlüsselung (CBC). Zu entschlüsseln auf <http://www.cryptool-online.org>
ZZZZZ UMKOD JSXCB QEHHX SQHJU BGJRR FIHMX KCJSM BCKDB OSBSS CMKEK
QESTX KGMRE JTETX FLDFM VHPJW QUXCV NDNUX ILKMC BEALA XDRUM JMPHT
WUKBL OSUUP ONUHA IGVIF GOKZZ YYYYY
Ende der verschlüsselten Nachricht

Fragen

1. Wer hat die AES-Verschlüsselung erfunden?
2. Kann jemand eine mit AES chiffrierte Botschaft ohne Schlüssel lesen?
3. Worin besteht das Problem, wenn man jemandem eine AES-Botschaft zukommen lassen will?

Antwort zu der Einstiegsfrage

Kann eine Botschaft sicher verschlüsselt werden?

Die AES-Verschlüsselung gilt momentan als sehr sicher. Eine Problematik bei der symmetrischen Verschlüsselung besteht darin, dass die empfangende Person den Schlüssel zum Dechiffrieren braucht und dieser sicher übermittelt werden muss.

Beim obigen Beispiel wird die Webanwendungen der Webseite <http://www.cryptool-online.org> benutzt, um den AES-Algorithmus ohne Installation von Software zu demonstrieren. Dabei wird erstens die Botschaft über einen unsicheren Kanal und zweitens an einen fremden Server geschickt. Dieses Vorgehen ermöglicht es, einen Text mit AES zu verschlüsseln, jedoch nicht auf eine sichere Weise.

Wenn immer Daten und Informationen an eine Webseite geschickt werden, kennt der Webseitenbetreiber die übermittelten Inhalte. Deshalb sollten auf keinen Fall echte Geheimnisse, wie z.B. aktuelle Passwörter, an eine Webseite gesendet werden.

Für den Fall, dass Inhalte auf einem Computer sicher verschlüsselt werden sollen, kann die Open Source Software OpenSSL verwendet werden. In einem Terminalfenster kann mithilfe der folgenden Kommandozeile ein Text, z.B. mit dem Namen *MeinText.txt*, in einen mit AES verschlüsselten Geheimtext, z.B. *GeheimText.enc*, chiffriert werden.

Kommandozeile:

```
openssl aes-256-cbc -in MeinText.txt -out GeheimText.enc
```

- Für die Betriebssysteme Linux und OS X ist OpenSSL vorinstalliert.
- Für Windows-Systeme muss OpenSSL selbstständig installiert werden, z.B. <http://gnuwin32.sourceforge.net/packages/openssl.htm>