Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
13. Januar 2010

Entschlüsselung geheimer Botschaften am Computer
Anleitung

Allgemeines: Dieser Workshop wurde im Schülerseminar in 90 Minuten durchgeführt. Die Zeit hat gut gereicht. Da nur 90 Minuten zur Verfügung standen, habe ich viel auf die Arbeitsblätter geschrieben, damit die Schülerinnen und Schüler wenig Zeit zum Mitschreiben brauchten.

Das Material wurde zum Teil an der Tafel und zum Teil mit dem Beamer praesentiert, so wie im Text angegeben.

Es werden die Verschlüsselungen *Cäsar, Substitution, Vigenère* und *Hill* besprochen und verschlüsselte Texte entschlüsselt. Die ersten drei Verfahren können durch Häufigkeitsanalyse geknackt werden. Das Hillsche Verfahren ist das erste, das einen mathematischen Algorithmus benützt, und kann nicht durch Häufigkeitsanalyse geknackt werden. Trotzdem hat es keine Bedeutung erlangt, da die Vorlage nur eines Textes in ver- und entschlüsselter Form genügt, um die zur Entschlüsselung jedes weiteren genauso codierten Textes nötigen Parameter zu bestimmen. An moderne Verfahren wird der viel höhere Anspruch gestellt, dass selbst bei Vorliegen von mehreren ver- und entschlüsselten Texten die Verschlüsselungsparameter nicht herausgefunden werden können.

Alle für den Workshop verwendeten Dateien sind im Verzeichnis kryptographie enthalten.

Ich habe die Erfahrung gemacht, dass hin und wieder aus Versehen geänderte Texte von den Schülerinnen und Schülern abgespeichert werden. Daher habe ich es auf unseren Computern so eingerichtet, dass die Schüler nach dem Einloggen ein Startprogramm (`workshop`) aufrufen, das alle lokal vorhandenen Dateien löscht, dann von einem zentralen Rechner die Originaldateien kopiert und erst dann die beiden zum Entschlüsseln nötigen Programme startet. So kann man im Notfall einfach die Programme beenden und neu das Startprogramm aufrufen. Alternativ kann man auf jedem Rechner ein Unterverzeichnis anlegen, in dem die Originaldateien liegen und sie dann von dort kopieren.

Für den Workshop habe ich das Programm `cryptool` und den Editor `emacs` verwendet. Man kann auf den `emacs` verzichten, aber ich finde den Entschlüsselungsmodus im `emacs` sehr schön. `cryptool` ist ein freies Windows-Programm und kann von `http://www.cryptool.de/` heruntergeladen werden. Auf unseren Linux-Rechnern läuft es mit `wine`. Den ebenfalls freien Editor `emacs` gibt es für viele Betriebssysteme (auch für Windows), bei Linux ist er standardmäßig dabei.

Arbeitsblatt 1: Die Arbeitsblätter stehen ab Seite 4 in der originalen Fassung, wie ich sie ausgeteilt habe.

Nach Austeilen des Arbeitsblattes habe ich mich wie angegeben eingeloggt und auf dem Beamer gezeigt, wie der Bildschirm dabei aussieht. Parallel dazu haben sich die Schüler eingeloggt. Dann habe ich auf der Tafel kurz einen Teil der angegebenen Tabelle angeschrieben und erklärt, wie die Cäsar-Verschlüsselung funktioniert. Dann sollten sie Schüler auf das Arbeitsblatt über die Geheimbotschaft den entschlüsselten Text schreiben. Währenddessen habe ich den verschlüsselten Text an die Tafel geschrieben und dann die von den Schülern gelieferte Lösung drübergeschrieben.
(Lösung: GUMMIBAERCHEN SCHMECKEN GUT)

Vielleicht kommt von den Schülern die Frage, warum nur 25 Möglichkeiten durchprobiert werden müssen, obwohl das Alphabet 26 Buchstaben hat.

Hier folgte der Hinweis, dass man lieber ein Programm probieren lässt als dies von Hand zu tun. Auch die Entschlüsselung geht dann schneller.

Dann habe ich wieder vorgemacht, wie man in `cryptool` und im `emacs` Dateien öffnet und den Entschlüsselungmodus einstellt. Beim ersten Text findet `cryptool` problemlos die Lösung. Aber beim zweiten Text kommt nichts gescheites heraus. Er ist zu kurz und hat nicht die richtigen Buchstabenhäufigkeiten. Hier muss man wirklich im `emacs` herumprobieren.

Arbeitsblatt 2: Hier habe ich an der Tafel die Cäsar-Verschlüsselungszeile unter dem Alphabet weggewischt, eine beliebige Permutation druntergeschrieben und erklärt, wie man verschlüsselt. Dann noch ein paar Worte zu den Häufigleitstabellen auf der Rückseite des Arbeitsblattes, und schon gings los mit dem Probieren. Bei Fragen habe ich meist am Beamer erklärt, wie man es macht, damit auch die Mitschüler von der Antwort profitieren konnten. Die Texte sind verschieden schwierig zu entschlüsseln. Bei `text3` sind Abstände zwischen den Worten, das vereinfacht die Sache wesentlich. Bei `text4` sind die Wortabstände weggelassen. Dadurch ist die Entschlüsselung viel schwerer. Ich habe auf dem Arbeitsblatt als Hilfe den Anfang des entschlüsselten Textes angegeben, weil wir nicht so viel Zeit hatten. Wenn genug Zeit vorhanden ist, kann man diesen Hinweis weglassen. Diejenigen, die mit der Entschlüsselung schnell fertig waren, habe ich gefragt, aus welchen Büchern ich die Texte entnommen habe.

Arbeitsblatt 3: Hier habe ich die erste Seite mit dem Beamer gezeigt und erklärt, wie man den angegebenen Satz *Heute ist es sehr heiss* verschlüsselt: Man schreibt das Schlüsselwort unter den Klartext. Dann sucht man in der Spalte, in der oben der Klartextbuchstabe steht, die Zeile, in deren Anfang der enstprechende Buchstabe des Schlüsselwortes steht und liest den Eintrag ab. Dies ist der verschlüsselte Buchstabe. Am Beispiel:

Unter „H“ steht „p“, dann wird „H“ mit der „p“-Zeile verschlüsselt: H→w.
Unter „E“ steht „r“, dann wird dieses „E„ mit der „r“-Zeile verschlüsselt: E→v.

Nun sollte man ein Säckchen Gummibären zur Hand haben, denn der entschlüsselte Text lautet: KANN ICH BITTE EIN GUMMIBAERCHEN BEKOMMEN.

Hier kann man darauf hinweisen, dass die Verschlüsselungsmaschine Enigma etwas ähnliches gemacht hat.

Der verschlüsselte Text `text5` wurde mit dem Schlüsselwort *mathematik* verschlüsselt. Dies bekommt `cryptool` problemlos heraus.

Arbeitsblatt 4: Hier muss mehr an der Tafel erklärt werden. Kurz gesagt, werden gleich lange Blöcke des Textes mit einer Matrix multipliziert und dann modulo 26 gerechnet. Ich habe an der Tafel erklärt, wie man zu dem Chiffretext kommt:

a) Man teilt den Text in Zweierblöcke auf. Da die Nachricht eine ungerade Anzahl von Buchstaben hat, ergänzt man einen zufälligen Buchstaben. Hier habe ich A an den Text angefügt:

$$6\ \ 4\,|\,7\ \ 4\,|\,8\ \ 12\,|\,1\ \ 14\,|\,19\ \ 18\,|\,2\ \ 7\,|\,0\ \ 5\,|\,19\ \ 0\,|$$

b) Dann berechnet man den Chiffretext paarweise.

Für das erste Paar $\begin{pmatrix} 3 & 24 \\ 25 & 1 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 4 \end{pmatrix}$:

1. Zeile der Matrix „mal“ Zahlenpaar: $3 \cdot 6 + 24 \cdot 4 = 114 \equiv 10 \mod 26$
2. Zeile der Matrix „mal“ Zahlenpaar: $25 \cdot 6 + 1 \cdot 4 = 154 \equiv 24 \mod 26$

Für das nächste Paar $\begin{pmatrix} 3 & 24 \\ 25 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix}$:

1. Zeile der Matrix „mal“ Zahlenpaar: $3 \cdot 7 + 24 \cdot 4 = 117 \equiv 13 \mod 26$
2. Zeile der Matrix „mal“ Zahlenpaar: $25 \cdot 7 + 1 \cdot 4 = 179 \equiv 23 \mod 26$

Die Entschlüsselung funktioniert genauso, aber mit einer anderen Matrix, die genau zur ursprünglichen passen muss. Mit der Entschlüsselungsmatrix auf dem Aufgabenblatt erhält man für den wieder in Zweierblöcke unterteilten Chiffretext

$$10 \quad 24 \,|\, 13 \quad 23 \,|\, 0 \quad 4 \,|\, 1 \quad 13 \,|\, 21 \quad 25 \,|\, 18 \quad 5 \,|\, 16 \quad 5 \,|\, 5 \quad 7 \,|$$

für das erste Paar $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 24 \end{pmatrix}$:

1. Zeile der Matrix „mal“ Zahlenpaar: $1 \cdot 10 + 2 \cdot 24 = 58 \equiv 6 \mod 26$
2. Zeile der Matrix „mal“ Zahlenpaar: $1 \cdot 10 + 3 \cdot 24 = 82 \equiv 4 \mod 26$

Für das nächste Paar $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 23 \end{pmatrix}$:

1. Zeile der Matrix „mal“ Zahlenpaar: $1 \cdot 13 + 2 \cdot 23 = 59 \equiv 7 \mod 26$
2. Zeile der Matrix „mal“ Zahlenpaar: $1 \cdot 13 + 3 \cdot 23 = 82 \equiv 4 \mod 26$

Hinweise: Das Programm `cryptool` gibt die transponierte Matrix an. Ich wollte aber hier die „normale“ Multiplikation einer Matrix mit einem Vektor verwenden, daher habe ich die im Programm verwendeten Matrizen transponiert. Außerdem ist die Erklärung im Programm falsch. Man kann bei einer Hill-Verschlüsselung ankreuzen, dass man die Details der Schlüsselmatrix angezeigt bekommt. Die Erklärung, die hier für die Multiplikation gegeben wird, ist zum Teil falsch.

Hier habe ich angemerkt, dass man bei diesem Programm auch größere Matrizen verwenden kann. Dann bringt Häufigkeitsanalyse überhaupt nichts. Trotzdem wurde dieses Verfahren nie verwendet, da man die Matrix berechnen kann, sobald ein ver- und entschküsselter Text vorliegt. Es gibt inzwischen Verfahren, bei denen nicht einmal die Kenntnis einiger ver- und entschlüsselter Texte zum Entschlüsselungscode verhilft.

Nun können die Schüler `text6` entschlüsseln.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
13. Januar 2010

Entschlüsselung geheimer Botschaften am Computer
Arbeitsblatt 1

Einloggen: Auf dem Login-Fenster die Nummer des Rechners ablesen, z.B. `stud29`. Als Login `guest` direkt gefolgt von der Nummer eingeben, also im Beispiel `guest29`. Als Passwort ... eintragen, dann mit der Eingabetaste bestätigen.

Ausloggen: Auf Hintergrund rechte Maustaste, untersten Punkt `Abmelden` auswählen.
Im Notfall: Die Tastenkombination strg-alt-⇐ beendet die Sitzung.

Öffnen der Programme: Falls nach dem Einloggen kein Arbeitsfenster erscheint, unten auf der Leiste auf das Bildschirm-Symbol klicken, dann wird ein Arbeitsfenster geöffnet. Falls beim Einloggen zwei Arbeitsfenster erscheinen, bitte eines wegklicken. Im Arbeitsfenster `workshop` eintippen und mit der Eingabetaste bestätigen. Dann dauert es kurz und zwei Fenster werden geöffnet. Das eine ist der *Emacs* (ein Editor), das andere *cryptool* (ein Schulungsprogramm zur Verschlüsselung).

Geheimbotschaft: `k y q q m f e i v g l i r  w g l q i g o i r  k y x`

Cäsar-Chiffre: Das Alphabet wird verschoben:

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Chiffretext:	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

Verschlüsselung knacken: Durchprobieren (25 Möglichkeiten)

Aufgabe: Entschlüssle die angegebene Geheimbotschaft und die Texte aus den Dateien `text1-Caesar.txt` und `text2-Caesar.txt`.

Cäsar-Chiffre knacken mit cryptool:

- Datei öffnen: `Datei`→`öffnen` anklicken, dann Datei auswählen und `open` anklicken.
- `Analyse`→`Algorithmen (automatische Analyse)`→`Caesar` anklicken.
  Bei jeder Anfrage bestätigen, dann erscheint der entschlüsselte Text.

Cäsar-Chiffre knacken mit emacs:

- Datei öffnen: `File`→`Open File` anklicken, dann zweimal die Tabulator-Taste drücken. Das Fenster teilt sich, in der unteren Hälfte erscheint eine Auswahl. Den gewünschten Text mit mittlerer Maustaste auswählen.
- In den Entschlüsselungsmodus gehen: Die Tastenfolge Alt-`x decipher` gefolgt von der Eingabetaste schaltet in den Entschlüsselungsmodus. Nun kann direkt auf den Großbuchstaben der vermutete zugehörige entschlüsselte Buchstabe eingegeben werden.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
13. Januar 2010

Entschlüsselung geheimer Botschaften am Computer
Arbeitsblatt 2

Substitutionsverschlüsselung:

Klartext:	A	B	C	D	E	F	G	...	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
Chiffretext:	willkürlich vertauschte Reihenfolge										

Verschlüsselung knacken: Durch Häufigkeitsanalyse des Textes.

- Der häufigste Buchstabe in deutschen Texten ist „e“ mit 17,4%.
- Die beiden häufigsten Digramme (Buchstabenpaare) sind „er“ (4,1%) und „en“ (4,0%).
- Man kann noch die Häufigkeit der Trigramme (Dreierkombinationen von Buchstaben) zu Hilfe nehmen.

⟶ Rückseite.

Man nennt diese Verschlüsselungen „Monoalphabetische Substitutionen“

Aufgabe: Entschlüssle die Texte in den Dateien `text3-Substitution.txt` und `text4-Substitution.txt`.
Hinweis für die Datei `text4-Substitution.txt`: Der zugehörige Klartext beginnt mit „Ichglaubedass“.

Substitution-Chiffre knacken mit cryptool und emacs: `Cryptool` wird zur Textanalyse benutzt, `emacs` zur Eingabe der Entschlüsselung.

- In `Cryptool` die Chiffredatei öffnen.
- Dann mit `Analyse→Allgemein→N-Gramm` ein Histogramm (Häufigkeit der Buchstaben) erstellen und abspeichern. Jetzt sind zwei Fenster in `Cryptool` offen.
- Auf das Fenster mit der Chiffredatei klicken, damit dieses Fenster wieder das aktive wird. Dann mit `Analyse→Allgemein→N-Gramm` die Häufigkeit der Digramme berechnen und speichern.
- Auf das Fenster mit der Chiffredatei klicken, dann mit `Analyse→Allgemein→N-Gramm` die Häufigkeit der Trigramme berechnen und speichern.

Nun kann man mit den auf der Rückseite dieses Blattes angegebenen Häufigkeitsverteilungen anfangen, die Bedeutung der Buchstaben zu erraten.

Zum Entschlüsseln: Im `emacs` dieselbe Chiffredatei wie in `Cryptool` öffnen (`File→Open File` anklicken, dann zweimal die Tabulator-Taste drücken. Das Fenster teilt sich, in der unteren Hälfte erscheint eine Auswahl. Den gewünschten Text mit mittlerer Maustaste auswählen). Dann ist der verschlüsselte Text im Editor. Nun die Tastenfolge Alt`-x decipher` gefolgt von der Eingabetaste eingeben. Dann ist der Editor im Entschlüsselungsmodus. Die großgeschriebenen Buchstaben sind die des verschlüsselten Textes, die kleingeschriebenen die des entschlüsselten Textes. Nun können auf dem großgeschriebenen Alphabet Kleinbuchstaben eingegeben werden. Diese werden dann daruntergeschrieben und im Text entsprechend ersetzt.

Häufigkeitsverteilungen in deutschsprachigen Texten

Buchstaben		Buchstaben	
E	17,40 %	M	2,53 %
N	9,78 %	O	2,51 %
I	7,55 %	B	1,89 %
S	7,27 %	W	1,89 %
R	7,00 %	F	1,66 %
A	6,51 %	K	1,21 %
T	6,15 %	Z	1,13 %
D	5,08 %	P	0,79 %
H	4,76 %	V	0,67 %
U	4,35 %	J	0,27 %
L	3,44 %	Y	0,04 %
C	3,06 %	X	0,03 %
G	3,01 %	Q	0,02 %

Digramme

ER	4,09 %
EN	4,00 %
CH	2,42 %
DE	1,93 %
EI	1,87 %
ND	1,85 %
TE	1,68 %
IN	1,63 %
IE	1,47 %
GE	1,40 %
ES	1,22 %
NE	1,19 %
UN	1,16 %
ST	1,12 %
RE	1,02 %
HE	1,02 %
AN	1,02 %
BE	1,01 %

Trigramme

EIN	1,22 %
ICH	1,11 %
NDE	0,89 %
DIE	0,87 %
UND	0,87 %
DER	0,86 %
CHE	0,75 %

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
13. Januar 2010

Entschlüsselung geheimer Botschaften am Computer
Arbeitsblatt 3

Die Vigenère Verschlüsselung, eine polyalphabetische Substitution:

Vigenère-Quadrat:

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

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Schlüsselwort „primzahl“:

Klartext:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Chiffretext:	w	v	c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a

Aufgaben: 1) Entschlüssle mit dem Schlüsselwort „handy“ den Text

r a a q g j h o l r a e r l l n u z p g i a r u a o e a e c r o z p c u

2) Entschlüssle den Text aus der Datei `text5-Vigenere.txt` mit Hilfe des im Programm `cryptool` eingebauten Analyse-Algorithmus.

Anmerkungen:

Vorteil: Die Buchstabenhäufigkeit ist versteckt. Gleiche Buchstaben werden verschieden verschlüsselt

Nachteil: Nach l Buchstaben (l =Länge des Schlüsselwortes) wiederholt sich die Verschlüsselung, jeder Block aus l Buchstaben wird nach dem gleichen Prinzip verschlüsselt

Vigenère-Verschlüsselung knacken:

- Finde die Länge l des Passwortes
- Schreibe den verschlüsselten Text in l Spalten
- In jeder Spalte Häufigkeitsanalyse liefert die Codierung von „E“

Dann ist das Schlüsselwort bekannt, der Text kann entschlüsselt werden.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
13. Januar 2010

Entschlüsselung geheimer Botschaften am Computer
Arbeitsblatt 4

Die Hill-Verschlüsselung, ein linearer Code:

Benötigt: Eine Nummerierung des Alphabets

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

und ein quadratisches Zahlenschema („Matrix“), z.B. $\begin{pmatrix} 3 & 24 \\ 25 & 1 \end{pmatrix} = \begin{pmatrix} \mathrm{D} & \mathrm{Y} \\ \mathrm{Z} & \mathrm{B} \end{pmatrix}$.

Verschlüsselung:

Klartext:	G	E	H	E	I	M	B	O	T	S	C	H	A	F	T	A
	6	4	7	4	8	12	1	14	19	18	2	7	0	5	19	0
Chiffretext:	k	y	n	x	a	e	b	n	v	z	s	f	q	f	f	h
	10	24	13	23	0	4	1	13	21	25	18	5	16	5	5	7

Entschlüsselung: Im Beispiel mit der Matrix $\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} \mathrm{B} & \mathrm{C} \\ \mathrm{B} & \mathrm{D} \end{pmatrix}$

Aufgabe: Entschlüssle den Text aus der Datei `text6-Hill.txt` mit Hilfe des Analyse-Algorithmus aus `cryptool`.
Hinweis: Der zugehörige Klartext beginnt mit „`dermysterioesemrthorndike`“
Achtung: Das Programm cryptool schlägt einen Schlüssel vor. Diesen Schlüssel notieren und das zugehörige Fenster schließen, sonst stürzt das Programm ab. Dann kann mit dem Schlüssel unter `Ver-/Entschlüsseln` der text entschlüsselt werden.

Hinweise: Das Programm `cryptool` kann für Windows heruntergeladen werden von `http://www.cryptool.de/`

Den Editor `Emacs` gibts auch für Windows zum runterladen (selber suchen).

Eine sehr schöne Seite über Verschlüsselung findet sich unter
`http://delphi.zsg-rottenburg.de/krypt.html`