FACHHOCHSCHULE **TRIER**
Hochschule für Technik, Wirtschaft und Gestaltung
University of Applied Sciences
Informatik

Anleitung für das Programm der klassichen Chiffre

Stephan Simons

Programmhilfe

Betreuer: Prof. Dr. Alfred Scheerhorn

Trier, 16.05.2006

Inhaltsverzeichnis

1

Einleitung

Dieses Handbuch beschreibt die Benutzung des Programmes.

Bereits die Ägypter nutzten um 1900 vor Christus die Kunst einen Text zwischen Sender und Empfänger zu verschlüsseln, damit ein Dritter diesen nicht lesen konnte.

Die erstellte Software soll die Analyse von Texten und Chiffrierung bzw. Dechiffrierung erleichtern. Die zeitaufwändigen Vorgänge, wie beispielsweise Buchstabenhäufigkeiten ermitteln, übernimmt das Programm. Die lästigen Arbeiten brauchen nun also nicht mehr selber vorgenommen zu werden. Das erhöht die Motivation.

Im Kapitel 2 dieser Ausarbeitung befindet sich die Problemstellung. Dazu wird ein bekanntes Programm auf dem Gebiet der Kryptographie und dessen Nachteile kurz vorgestellt. Anschließend wird die genaue Aufgabenstellung dieses Projektes erläutert.

Das 3. Kapitel gibt dem Leser eine Einführung in die Thematik der klassischen Chiffren. Dazu werden alle für das Projekt relevanten Chiffren angesprochen und soweit sinnvoll, auch passende Beispielen angegeben. Die beiden wichigsten Inhalte sind die Substitutions- und polyalphabetischen Chiffren. Daraufhin werden die Kryptoanalyse-Vorgehensweisen der vorgestellten Chiffren besprochen.

Hauptbestandteil des Handbuchs ist das Anwenderhandbuch. Es gibt dem Benutzer eine Hilfe bei der Benutzung des Programms. Dazu werden die ersten Schritte beschrieben und auch Analyse- sowie Chiffrierungsfunktionen.

2

Einführung in die klassische Kryptographie

Das folgende Kapitel gibt einen Überblick über klassische Verfahren der Kryptographie. Dazu werden additive und linear affine Chiffren vorgestellt und die Besonderheit bei der Schlüsselwahl der linear affinen Chiffre. Im Anschluss folgt eine Erklärung der Vignère-, Beaufort-Chiffren. Zum Schluss des Kapitels wird eine besondere Form der Vignère-Chiffren vorgestellt, die mit einer linear affiner Verschlüsselung funktioniert.
Um das Verständnis der Chiffren zu verbessern, wurde möglichst zu jeder Chiffre ein Beispiel gewählt.

2.1 Additive Chiffren

Bei den additiven Chiffren wird das zu verschlüsselnde Zeichen um b Stellen im gegebenen Alphabet weitergeschoben. Zur mathematischen Darstellung der Verschlüsselung werden den Buchstaben die Zahlen 0 bis 25 zugeordnet. Abbildung 3.1 zeigt eine solche Zuordnung von Zeichen zu Zahlen bei einer Alphabetgröße(n) = 26:

Zeichen	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
Nummer	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

Abbildung 2.1. Tabelle: Grossbuchstaben und ihre Stelle im Alphabet

Um sicherzustellen, dass die chiffrierte Zahl ebenfalls im Alphabet vorhanden ist, sollte das Ergebnis zyklisch weitergeschoben werden.

Die Verschlüsselung eines Klartextzeichens q ist gegeben durch

$$c \;=\; q + b \; mod \; n \tag{2.1}$$

Das dazu entsprechende Zeichen kann aus der obigen Tabelle entnommen werden.

Analog dazu erfolgt die Entschlüsselung durch die Berechnung

$$q \;=\; c - b \; mod \; n \tag{2.2}$$

Beispiel:

```
Alphabetgröße         : 26
verwendeter Schlüssel: 'D' entspricht 3

Zu verschlüsseln      :  'H'  'A'  'U' 'S'
numerische Werte      :   7    0   20  18

Verschlüsselt         :  10    3   23  21
Verschlüsselter Text  :  'K'  'D'  'X' 'V'
```

Additive Chiffre werden auch Cäsar-Chiffre genannt.

2.2 Linear affine Chiffren

Affine Chiffren sind den additiven sehr ähnlich. Sie benutzen jedoch noch einen multiplikativen Faktor a. Der Schlüssel besteht bei affinen Chiffren also aus einem Tupel (a,b).

Die Verschlüsselung affiner Chiffren erfolgt mit

$$c \;=\; (a * q) \;+\; b \; mod \; n \tag{2.3}$$

Analog dazu wird die Entschlüsselung:

$$q \;= \frac{(c-b)}{a} \; mod \; n \tag{2.4}$$

Zulässig sind nur Werte, die teilerfremd zu n sind. Daher stehen für den multiplikativen Schlüssel nicht alle Elemente aus dem Alphabet zur Verfügung.

Beispiel:

```
Alphabetgröße                 : 26
additiver  Schlüssel (b)      : 'F' entspricht 5
multiplikativer Schlüssel (a): 'D' entspricht 3

Zu verschlüsseln      :  'H'  'A'  'U' 'S'
numerische Werte      :   7    0   20  18

Verschlüsselt         :   0    5   13   7
Verschlüsselter Text  :  'A'  'F'  'N' 'H'
```

2.2.1 Berechnung multiplikativer Inverse modulo Alphabetgröße

Die Anzahl der für die Verschlüsselung verwendbaren Faktoren a kann mit der Eulerschen Φ-Funktion die Anzahl der teilerfremden Zahlen zwischen 1 und n berechnet werden.

Das multiplikative Inverse z einer zu n teilerfremden Zahl x läßt sich mit dem Satz von Euler berechnen durch

$$z \;=\; x^{\Phi(n)-1} \; mod \; n \tag{2.5}$$

Die Voraussetzung für die Nutzung des Euler-Satzes besteht darin, dass x teilerfremd zu n ist.

2.3 Vignère-Chiffre

Vignère-Chiffre erweitern die additiven Chiffre. Sie verwenden statt einem einzelnen Zeichen b als Schlüssel eine Zeichenkette $b_0 \ldots b_{k-1}$ für $k > 0$. In Kapitel 3.5 ist eine spezielle Variante der Vignère-Chiffren beschrieben, die zusätzlich einen multiplikativen Schlüssel nutzt.

Beispiel: Verschlüssele 'HERZKOENIG' mit dem Schlüssel 'DAME'

```
Alphabetgröße         : 26
verwendeter Schlüssel:  'D'  'A'  'M'  'E'  'D'  'A'  'M'  'E'  'D'  'A'
numerische Werte      :   3    0   12    4    3    0   12    4    3    0

Zu verschlüsseln      :  'H'  'E'  'R'  'Z'  'K'  'O'  'E'  'N'  'I'  'G'
numerische Werte      :   7    4   17   25   10   14    4   13    8    6

Verschlüsselt         :  10    4    3    3   13   14   16   17   11    6
Verschlüsselter Text  :  'K'  'E'  'D'  'D'  'N'  'O'  'Q'  'R'  'L'  'G'
```

2.4 Beaufort-Chiffre

Beaufort-Chiffre unterscheiden sich von den Vignère-Chiffre nur in der verwendeten Berechnungform. Als additiven Schlüssel wird eine Zeichenfolge $b_0 \ldots b_{k-1}$ für $k > 0$ benötigt.
Bei den Beaufort-Chiffren wird das Klartextzeichen von dem Schlüsselzeichen subtrahiert.Damit entspricht die Verschlüssellung der Entschlüsselung.

$$c \;=\; b - q \; mod \; n \tag{2.6}$$

Beispiel: Verschlüssele 'HERZKOENIG' mit dem Schlüssel 'DAME'

```
Alphabetgröße         : 26
verwendeter Schlüssel:  'D'  'A'  'M'  'E'  'D'  'A'  'M'  'E'  'D'  'A'
numerische Werte      :   3    0   12    4    3    0   12    4    3    0

Zu verschlüsseln      :  'H'  'E'  'R'  'Z'  'K'  'O'  'E'  'N'  'I'  'G'
numerische Werte      :   7    4   17   25   10   14    4   13    8    6

Verschlüsselt         :   4    4    5   21    7   14   18    9    5    6
Verschlüsselter Text  :  'E'  'E'  'F'  'V'  'H'  'O'  'S'  'J'  'F'  'G'
```

2.5 Vignère-Chiffren mit linear affiner Verschlüsselung

Eine weitere Variante von kryptographischen Verfahren sind die Vignère-Chiffren, die zusätzlich zu ihren additen Schlüssel noch einen multiplikativen Schlüssel nutzen.
Die Berechnungsform der Verschlüsselung bzw. der Entschlüsselung entspricht der linear affinen Chiffren (siehe Kapitel 3.2). Allerdings wird als additiver Schlüssel b eine Zeichenkette b_0 ... b_{k-1} für $k > 0$ und als multiplikativer Schlüssel eine Zeichenkette a_0 ... a_{m-1} für $m > 0$ verwendet. Die Voraussetzung um den Text korrekt entschlüsseln zu können besteht darin, dass alle Zeichen a_0 ... a_{m-1} teilerfremd zu n sind. Die Länge der beiden Schlüssel kann unterschiedlich sein.

Beispiel: Verschlüssele 'HERZKOENIG' mit additiven Schlüssel 'DAME' und dem multiplikativen Schlüssel 'FHTR'

```
Alphabetgröße         : 26
Zu verschlüsseln      :  'H'  'E'  'R'  'Z'  'K'  'O'  'E'  'N'  'I'  'G'
numerische Werte      :   7    4   17   25   10   14    4   13    8    6

multipl. Schlüssel    :  'F'  'H'  'T'  'R'  'F'  'H'  'T'  'R'  'F'  'H'
numerische Werte      :   5    7   19   17    5    7   19   17    5    7

additiver Schlüssel   :  'D'  'A'  'M'  'E'  'D'  'A'  'M'  'E'  'D'  'A'
numerische Werte      :   3    0   12    4    3    0   12    4    3    0

Verschlüsselt         :  12    2   23   13    1   20   10   17   17   16
Verschlüsselter Text  :  'M'  'C'  'X'  'N'  'B'  'U'  'K'  'R'  'R'  'Q'
```

3

Kryptoanalyse klassischer Chiffren

Das Kapitel stellt die verschiedenen Analysemethoden vor, mit deren Hilfe additive, linear affine Chiffren, sowie Vignère- und Beaufort-Chiffren entschlüsselt werden könnnen. Zu Beginn des Kapitels werden jedoch allgemeinere Methoden der Kryptoanalyse wie z.B. der *ciphertext only attack* vorgestellt, die für die Entschlüsselung der Chiffren genutzt werden.

3.1 Allgemeine Methoden

In den allgemeinen Methoden werden die Verfahren *ciphertext only attack* und *known plaintext attack* erläutert.

3.1.1 ciphertext only attack

Die statistischen Eigenschaften der Buchstaben in der deutschen Sprache sind bekannt. Daher wird die Häufigkeitsanalyse genutzt, um einen Text zu entschlüsseln. Die Kryptoanalyse funktioniert folglich nur bei deutschen Texten. Des weiteren werden bei der Analyse die Bigramme und Trigramme berücksichtigt.
Oft vorkommende Zeichen im chiffrierten Text entsprechen mit einer hohen Wahrscheinlichkeit den in der deutschen Sprache häufig vorkommenden Zeichen.

Der *ciphertext only attack* liefert jedoch nur bei langen Texten ein korrektes Ergebnis. Weiterhin sollte die Auftrittswahrscheinlichkeit der einzelnen Zeichen nicht gleichverteilt sein, um ein gutes Resultat zu gewährleisten.

3.1.2 knwown plaintext attack

Wenn bereits Buchstabenzuordnungen von Chiffretextzeichen zu Klartextzeichen bekannt sind, kann die Menge der in Frage kommenden Schlüssel reduziert werden. Sind bereits d Buchstabenzuordnungen bei einer Alphabetgröße n bekannt, so bleiben lediglich (n-d)! Möglichkeiten übrig.

3.1.3 Chi-Quadrat-Abweichung

Der Chi-Quadrat-Wert, auch bekannt als *chiSquare* entspricht der Abweichung des Textes zur deutschen Sprache. Befindet sich der ermittelte Wert dieser Abweichung in einem gewissen, vorher festgelegten Spektrum, so kann davon ausgegangen werden, dass es sicht tatsächlich um einen deutschen Text handelt.
Leider lässt sich die Chi-Quadrat-Abweichung nach oben hin nicht genau begrenzen. Erfahrungswerte zeigen jedoch, dass das Maximum bei 300 erreicht ist. Typischerweise werden Werte zwischen 0 und 30 als sprachkonform angesehen. Aufgrund der unbekannen statistischen Zahlenverteilung werden Zahlen bei der Betrachtung ignoriert. Im Programm wurde es so realisiert, dass Groß- und Kleinbuchstaben dieselbe Auftrittswahrscheinlichkeit haben, um die Berechnungsform nicht unnötig zu verkomplizieren.

Die Chi-Quadrat-Abweichung wird mit der Alphabetgröße n und einer Auftrittwahrscheinlichkeit h_i eines Zeichens a_i und der Wahrscheinlichkeit eines Auftretens in der deutschen Sprache p_i ermittelt:

$$\sum_{a_i} (\frac{h_i}{n} - p_i)^2 \tag{3.1}$$

3.2 Entschlüsselung additiver Chiffren

Die additiven Chiffren besitzen lediglich n (n entspricht der Alphabetgröße) Schlüsselmöglichkeiten. Der Angreifer hat rechnergestützt wenig Aufwand einen *bruteforce*-Angriff durchzuführen. Dabei werden alle Schlüsselmöglichkeiten durchprobiert.

Eine andere Möglichkeit besteht darin, ein *ciphertext only attack* durchzuführen. Dazu sollten alle Häufigkeiten des chiffrierten Text ermittelt werden. Für die Entschlüsselung nutzt man die Eigenschaften der deutschen Sprache. So tritt das Zeichen E im deutschen zu rund 15 % auf. Die Wahrscheinlichkeiten können der Tabelle in Abbildung 4.2 entnommen werden.

*	15,15	0
E	15,35	18,10
N	8,84	10,42
R	6,86	8,08
I	6,38	7,52
S	5,39	6,35
T	4,73	5,57
A	4,58	5,40
D	4,39	5,17

Abbildung 3.1. Wahrscheinlichkeiten häufiger Buchstaben der deutschen Sprache

Beispiel für eine Kryptoanalyse additiver Chiffre:
Ist das häufigste Zeichen z.B. G im chiffrierten Text erkannt, so ist die Wahrscheinlichkeit hoch, dass die Differenz zwischen diesem zu dem Zeichen E der gesuchte Schlüssel ist: in dem Fall G - E = C
Zum Schluss kann mit der ChiSquare-Abweichung die Abweichung des Textes zur deutschen Sprache ermittelt werden.

In der erstellten Software wurde die vorgestellte Verschlüsselung implementiert. So werden die drei häufigsten Zeichen des Textes und deren Differenz im Alphabet zu einem Zeichen 'e' bzw. 'E' ermittelt. Diese drei Werte entsprechen bei einer hohen Buchstabenverteilung mit einer hohen Wahrscheinlichkeit den möglichen Schlüsseln. Das Programm entschlüsselt den Text mit disen drei möglichen Schlüssel und gibt die Resultate aus.

3.3 Entschlüsselung linear affiner Chiffren

Affine Chiffren besitzen insgesamt $n \cdot \Phi(n)$ Schlüsselmöglichkeiten. Ein rechnergestützter *bruteforce*-Angriff kann also problemlos durchgeführt werden.

Ähnlich wie bei den additiven Chiffren im vorherigen Kapitel kann ein *ciphertext only attack* mittels einer Häufigkeitsanalys durchgeführt werden. Die Zuordnung von Chiffre- zu Klartextzeichen erfolgt dann anhand der Auftrittswahrscheinlichkeit.

Weiterhin bietet sich ein *known plaintext attack* an, wobei die Entschlüsselung durch die zwei bekannte Paare ($q1$,$c1$) und ($q2$,$c2$) erfolgt. Dazu sollte die Differenz zwischen $q1$ und $q2$ jedoch modulo Alphabetgröße invertierbar sein (z.B. wenn $m1$ und $m2$ benachbart sind). Der multiplikative Schlüssel a entspricht

$$a \;=\; \frac{c1 - c2}{q1 - q2} \; mod \; n \tag{3.2}$$

Der additive Schlüssel (b) läßt sich mit

$$b \;=\; c1 - (q1 * a) \; mod \; n \tag{3.3}$$

berechnen.

In der erstellten Software wurden zwei Varianten implementiert.
Die erste Variante ist eine *bruteforce*-Methode. Um die Menge der Möglichkeiten einzuschränken wurden nur solche Schlüsselkombinationen zugelassen, die bei einer Dechiffrierung des häufigsten Kryptozeichens ein 'E' oder 'e' enthalten. Diese Auswahl wird weiter eingeschränkt, in dem alle entschlüsselten Texte mit einer Chi-Quadrat-Abweichung von über 30 ausgefiltert werden.
In der zweiten Variante wurde ein *known plaintext attack* realisiert. Dazu werden wahrscheinliche Kombinationsmgölichkeiten ausprobiert. Als Klartextzeichen dienen die in der deutschen Sprache häufig vorkommenden Zeichen *'e','n','r','i','s'*.

Die Dechiffrierung erfolgt durch die Auswahl 2er Zeichen aus den 5 (entspricht 6 Möglichkeiten), die auf die drei häufigsten Zeichen des chiffrierten Textes abgebildet werden. Somit ergeben sich insgesamt 60 Kombinationsmgöglichkeiten, die mit Hilfe der in 4.2 und 4.3 vorgestellten Berechnungsform analysiert werden können. Die Differenz der Klartextzeichen sollte eine multiplikative Inverse modulo Alphabetröße besitzen. Der Text wird mit den ermittelten Schlüsseln dechiffriert und anhand der Chi-Quadrat-Abweichung entschieden, ob der Text der deutschen Sprache entspricht und ausgegeben werden soll.

3.4 Vorgehen bei polyalphabetischen Chiffren

Polyalphabetische Chiffren sind den bereits vorgestellten Substitutionschiffren (additiv und linear affin) sehr ähnlich. Der größte Unterschied zwischen den Substitutionschiffren besteht darin, dass die polyalphabetische Variante statt einem einzigen Schlüsselzeichen eine Folge von Schlüsselzeichen verwendet.

Zuerst sollte die Schlüssellänge des Textes ermittelt werden. Dazu eignen sich die in Kapitel 4.5 und 4.6 vorgestellten Verfahren wie z.B. der Kasiski-Test oder die Berechnung des Koinzidenzindexwertes.

Daraufhin erfolgt nun die Auftrennung des Textes in Teilfolgen. Formal lässt sich Auftrennung wie folgt ausdrücken mit m als gewählte Teilfolgen:
$Text : z_1\ z_2 \quad z_3 \quad z_4 \quad z_5\ \ldots$

aufgespaltet in:

$$
\begin{array}{l}
z_1\ z_{1+m}\ z_{1+2\cdot m}\ z_{1+3\cdot m}\ z_{1+4\cdot m}\ \cdots \\
z_2\ z_{2+m}\ z_{2+2\cdot m}\ z_{2+3\cdot m}\ z_{2+4\cdot m}\ \cdots \\
. \\
. \\
z_m\ z_{2\cdot m}\ z_{3\cdot m}\ z_{4\cdot m}\ z_{5\cdot m}\ \cdots
\end{array}
$$

Dabei wird jedes Zeichen, das denselben Schluessel hat, untereinander geschrieben.

Beispiel einer Vignère-Chiffre bei ermittelter Schlüssellänge 4:

```
10    4    3    3
'K'  'E'  'D'  'D'

13   14   16   17
'N'  'O'  'Q'  'R'

11    6
'L'  'G'
```

Zum Schluss sollten die Teilfolgen wie in Kapitel 4.2 und 4.3 beschrieben, analysiert werden. Meistens liegt dem Text jedoch nur eine additive Chiffrierung zugrunde.

3.5 Kasiski-Test

Dieses Verfahren von Herr F.W. Kasiski beruht auf einem *ciphertext only attack*. Identische Klartextabschnitte werden in einem Text ermittelt. Mehrfach auftretende Zeichenfolgen legen die Vermutung nahe, dass sie mit demselben Schlüssel chiffriert wurden. Die Asbstände entsprechen dabei einem vielfachen der Schlüssellänge. Zur Analyse des Textes sollten alle Zeichenfolgen der Mindestlänge drei, sowie alle der Länge zwei mit einer Häufigkeit von mindestens drei verwendet werden. Die Angaben der Zeichenfolge und deren Abstände sollten aufgelistet und deren Teilerhäufigkeiten analysiert werden. Ein großer gemeinsame Teiler der Folge ist mit einer großen Wahrscheinlichkeit die gesuchte Teilfolge.

3.6 Koinzidenzindex

Der Wert dieses Indexes entspricht der Wahrscheinlichkeit, dass zwei unabhängig voneinander gewählte Zeichen des chiffrierten Textes übereinstimmen. Er kann zur Teilfolgenbestimmung genutzt werden.

In 4.4 wird die Berechnungsform des Koinzidenzindexes erläutert. Die Berechnung erfolgt mittels einer Summe über vorkommenden Zeichen des Textes. N entspricht der Textlänge, i dem aktuellen Zeichen des Textes und h_i die Auftrittswahrscheinlichkeit des Zeichens. Idealerweise wird dazu vorher eine Liste erstellt, welche die Häufigkeiten der einzelnen Textzeichen vermerkt.

$$\frac{\sum_i h_i \cdot (h_i - 1)}{N \cdot (N - 1)} \tag{3.4}$$

Der ermittelte Indexwert sollte nun mit der folgenden Tabelle in Abbildung 4.2 verglichen und der Wert mit der geringsten Abweichung gewählt werden. In der Überschrift sind die dazugehörigen Schlüssellängen angegeben.

Schlüssellänge	1	2	3	4	5	10	groß
Koinzidenzindex	0,076	0,057	0,051	0,048	0,046	0,042	0,038

Abbildung 3.2. Tabelle mit Koinzidenindexwerten und Teilfolgen

4

Anwenderhandbuch

Dieses Kapitel gibt dem Benutzer eine Hilfestellung bei der Benutzung der Software.

4.1 Allgemeines

Voraussetzung ist eine installierte, aktuelle Version der Java JRE. Das Sun Java Runtime Environment (JRE) in der Version 1.5.0 oder höher ist kostenlos unter [JavaSDK:1] zu beziehen. Ohne diese Java-Runtime-Programm kann das Kryptographie-Projekt nicht gestartet werden.

4.2 Erste Schritte

Wenn die jar-Datei gestartet wird, öffnet sich das Hauptfenster (Abbildung 5.1). Oben im Menü (siehe Punkt 1) im nachfolgenden Bild, sind alle Menüs bis auf das Menü Alphabet deaktiviert. Zu Beginn sollte der Menüeintrag Alphabet ausgewählt und entweder ein neues Alphabet erstellt oder ein bestehendes geöffnet werden. Nun öffnet sich ein Fenster mit einem Dialog, in dem alle Zeichen, die im

Abbildung 4.1. Startbildschirm

Alphabet vorhanden sein sollen, ausgewählt werden. Zulässig sind dabei Grossbuchstaben, Kleinbuchstaben und / oder Ziffern.
Wenn ein Alphabet ausgewählt wurde und daraufhin bestätigt wurde, sieht das Hauptfenster folgendermaßen aus (siehe Bild 5.2):

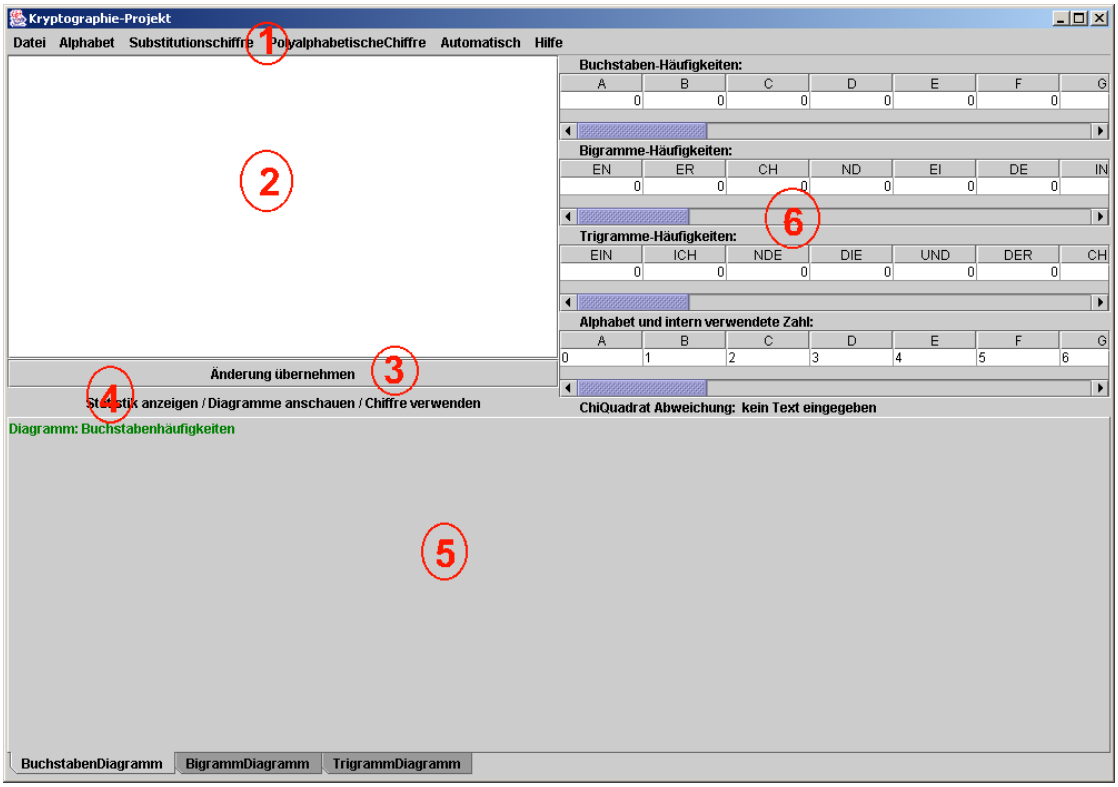

Abbildung 4.2. Hauptfenster

Erklärung:

1. Nun sind alle Menüeinträge aktiv und können ausgewählt werden.
2. Hier ist ein Textfeld, wo ein Text eingegeben werden kann. Dieser wird dann später von den jeweiligen Menüpunkten verwendet, um die Verschlüsselung/ Entschlüsselung durchzuführen. Alle Statistiken beziehen sich auf diesen Text.
3. Um Eingaben des Textfeld (2) zu übernehmen, damit die Statistiken aktualisiert werden können, sollte der Button *Änderungen übernehmen* geklickt werden.
4. Hier werden Informationen angezeigt, welche Aktionen vom Benutzer vogenommen werden sollen. Fehlermeldungen werden ebenfalls dort angezeigt.
5. Dieser Bereich steht erst zur Verfügung, wenn ein Alphabet ausgewählt wurde. Die Diagramme werden angezeigt, wenn Text in das Feld (1) eingegeben und mit dem entsprechenden Button (2) bestätigt wurde. Es zeigt dem Benutzer Diagramme über die Buchstabenverteilung an.
6. Ähnlich wie der Bereich mit den Diagrammen (5), steht das Feld erst nach Auswahl eines Alphabets zur Verfügung. Die Daten ändern sich automatisch, wenn ein Text eingegeben und bestätigt wurde.

Im Menü *Hilfe* befindet sich eine Information zum Programm und dessen Lizenz. Nun kann der Text aus dem Textfeld bearbeitet werden. Sie können dies entweder durch Eintippen in das Textfeld vornehmen, oder einen bestehenden Text öffnen. Dabei werden alle Zeichen, die dem Alphabet nicht angehören, ignoriert. Zu finden

ist der Dialog zum Öffnen einer Datei im Menü *Datei*. Dort gibt es außerdem die Möglichkeit einen Text zu speichern, das Textfeld zu löschen oder das Programm zu beenden.

ACHTUNG: Zu beachten ist, dass nur diejenigen Zeichen bei der Eingabe erlaubt sind, die im Alphabet ausgewählt sind.

Nachdem die Bearbeitung in dem Textfeld (2) erfolgte, sollte der Button *Änderungen übernehmen* geklickt werden. Nun zeigt sich im unteren Bereich des Fensters (5) ein sortiertes Diagramm der Buchstaben und ihren Häufigkeiten. An der untersten Programmleiste kann zwischen den Diagrammen des Typs Buchstaben, Bigramme, Trigramme ausgewählt werden. Die Tabelle zeigt genau wie die Diagramme die Zeichen des Alphabets, Bigramme und Trigramme und jeweils deren Häufigkeiten an. Dabei ist zu beachten, dass bei den Buchstabenhäufigkeiten alle Zeichen des Alphabets und deren Häufigkeiten angezeigt werden. Desweiteren sind die in der Tabelle gelisteten Bigramme und Trigramme einer Tabelle entnommen, die häufige Trigramme enthält. Wenn nun als Häufigkeit '0' angezeigt wird, deutet dies auf das fehlende Vorkommen der Zeichenfolge oder des Zeichnes im Text hin.

Unter der Tabelle wird noch die interne Zuweisung von Alphabetzeichen zur Zahl angezeigt. Darunter ist ein Feld, das die ChiQuadrat-Abweichung des Textes zur deutschen Sprache zeigt (siehe Kapitel 4.1.3).

Zum Schluss sollte das Hauptfenster in etwa so aussehen wie in Abbildung 5.3. Nun kann mit der Chiffrierung oder Dechiffrierung begonnen werden, die in den folgenden Kapitel beschrieben ist.

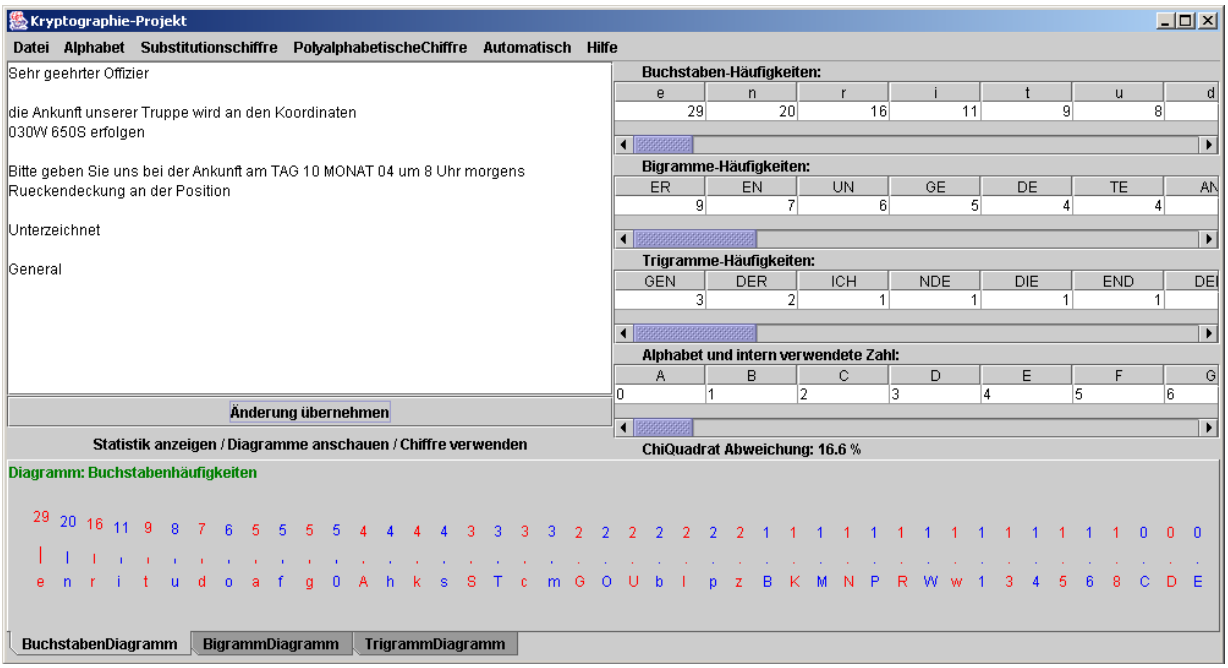

Abbildung 4.3. Hauptfenster nach der Eingabe

4.3 Menü Substitutionschiffre

Das Menü Substitutionschiffre umfasst folgende Chiffrierungs- und Dechiffrierungsmöglichkeiten:

- Additive Chiffre
- Affine Chiffre
- Substitutionen auf einen Text anwenden

Durch Auswahl des Menüeintrag öffnet sich das entsprechende Fenster.

4.3.1 Additive und affine Chiffren

Der Dialog der additiven und affinen Chiffren ähnelt sich. Exemplarisch wird in dieser Anleitung der Dialog der affinen Chifffren erläutert.
Anmerkung: Additive Chiffre entsprechen den affinen Chiffren mit einem multiplikativen Schlüssel a = **'B'** = 1.
Durch Auswahl des Menüeintrags *Affine Chiffre* öffnet sich das folgende Fenster:

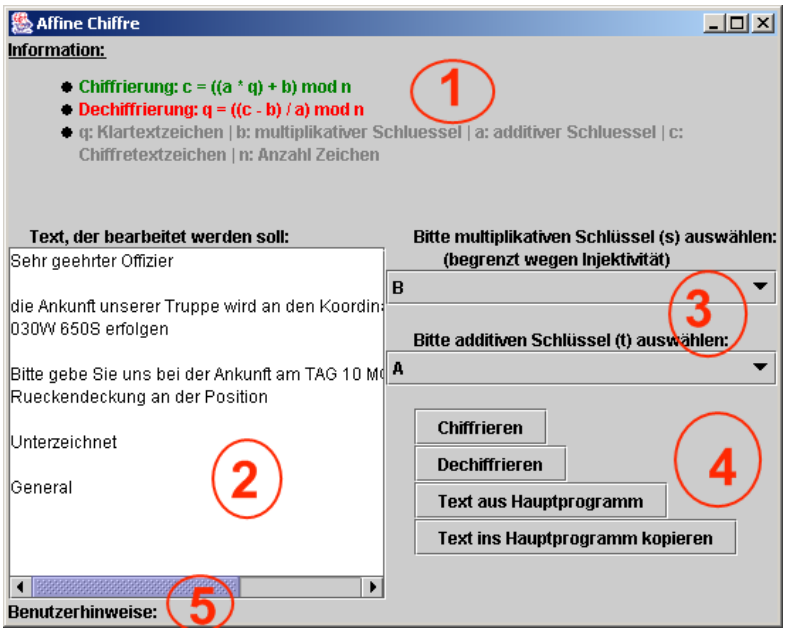

Abbildung 4.4. Dialog Affine Chiffre

Erklärung:

1. Informationen über den Chiffretyp und über Chiffrierung und Dechiffrierung
2. Textfeld, das zuerst Text aus Hauptfenster und nach der Chiffrierung/ Dechiffrierung den veränderten Text anzeigt.
3. Parameter für die Aktion. Hier werden die entsprechenden Schlüssel (additiv und ggf. multiplikativer) ausgewählt.
   Achtung: Als multiplikativer Schlüssel sind nur solche Zeichen zugelassen, die eine modulo Inverse besitzen (siehe Kapitel 4.2.1).

4. Folgende Buttons stehen zur Verfügung:
   - Chiffrieren
   - Dechiffrieren
   - Text aus Hauptprogramm
   - Text ins Hauptprogramm kopieren

   Die beiden oberen Funktionen führen mit den ausgewählten Schlüsseln (3) eine Chiffrierung/Dechiffrierung des Textes aus dem Textfeld (2) durch. Mit den letzen beiden Buttons kann ein Abgleich mit dem Hauptprogramm vorgenommen werden.
5. Anzeige von Informationen und Fehlermeldungen

Beispiel: Chiffrierung mit multiplikativem Schluessel a = '3' = 55 und additivem Schlüssel b = 'g' = 32:

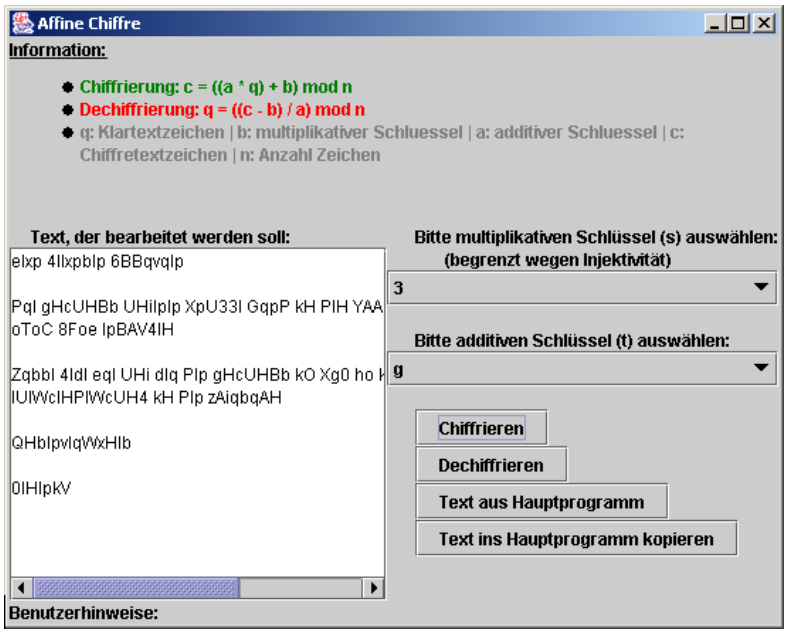

Abbildung 4.5. Dialog Affine Chiffre

4.3.2 Substitutionen auf einen Text anwenden

Mit dem Menüpunkt Substitutionschiffre können bestimmte Zeichen auf andere abgebildet werden. Das kann hilfreich sein, wenn man den Text analysieren will und schon Ideen hat, welche Zuordnungen passen könnten. Um eine Substitution hinzuzufügen, braucht der Benutzer lediglich das Zeichen *Von* auszuwählen, das auf das Zeichen *Nach* abgebildet werden soll und den Button *Zuweisung hinzufügen* anzuklicken. Substitutierte Zeichen werden im Text rot dargestellt.

Durch Auswahl des Menüeintrags *Substitutionschiffre* öffnet sich das folgende Fenster:

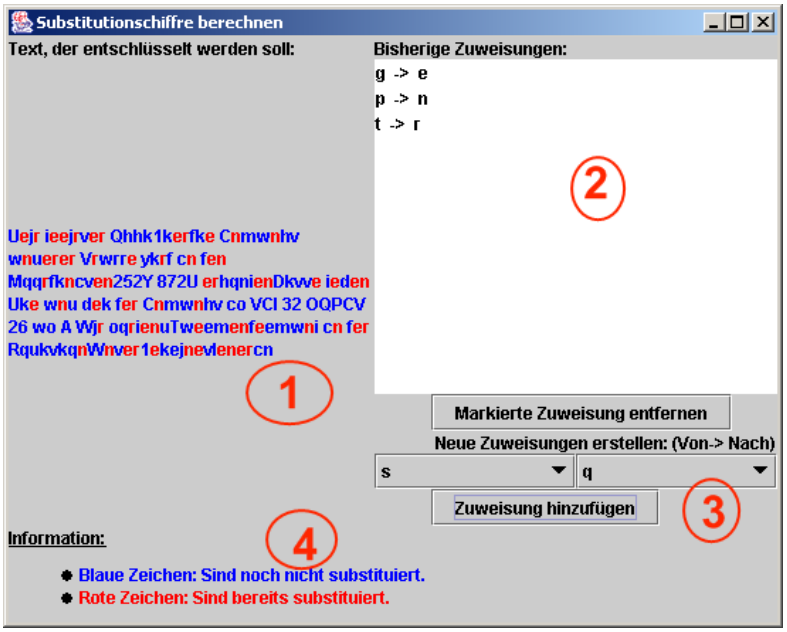

Abbildung 4.6. Dialog Substitutionschiffre

Erklärung:

1. Textfeld, das zuerst Text aus Hauptfenster und nach einer Substitution den veränderten Text anzeigt.
2. eine Liste mit allen bisher ausgewählten Substitutionen
3. Hier stehen dem Benutzer zwei Auswahlboxen zur Verfügung, um das Quell- und das Zielzeichen auszuwählen. Zwei Buttons zum Hinzufügen von diesen ausgewählten Substitutionen und zum Löschen eines ausgewählten Eintrags findet man dort ebenfalls. Wenn Sie eine bestehende Substitution gelöscht haben, wird der Text ohne diese Substitution angezeigt.
   Hinweis: Die Zeichen der zuvor gelöschgten Substitution werden ganz unten in die Auswahlboxen hinzugefügt.
4. Informationen

4.4 Menü Polyalphabetische Chiffre

Dieses Menü umfasst folgende Chiffrierungs- und Dechiffrierungsmöglichkeiten:

- Vignère-Chiffre
- Beaufort-Chiffre
- Kasiski-Test
- Koinzidenzindex berechnen

Über den entsprechenden Menüeintrag gelangen Sie in das jeweilige Fenster.

4.4.1 Vignère- und Beaufort-Chiffren

Die Dialoge für die Vignère- und Beaufort-Chiffre ähneln sich. Daher befindet sich in dieser Bedienunganleitung nur eine Beschreibung der Vignère-Chiffre.
Anmerkung: Im Fenster für die Vignère-Variante besteht im Gegensatz zu den Beaufort die Möglichkeit einen multiplikativen Schlüssel zu verwenden. Dieser String kann in ein entsprechendes Feld eingegeben werden. Es ist zu beachten, dass nur diejenigen Zeichen zur Auswahl stehen, die multiplikativ invertierbar modulo Alphabetgröße sind. Diese werden oben in den Informationen angezeigt.

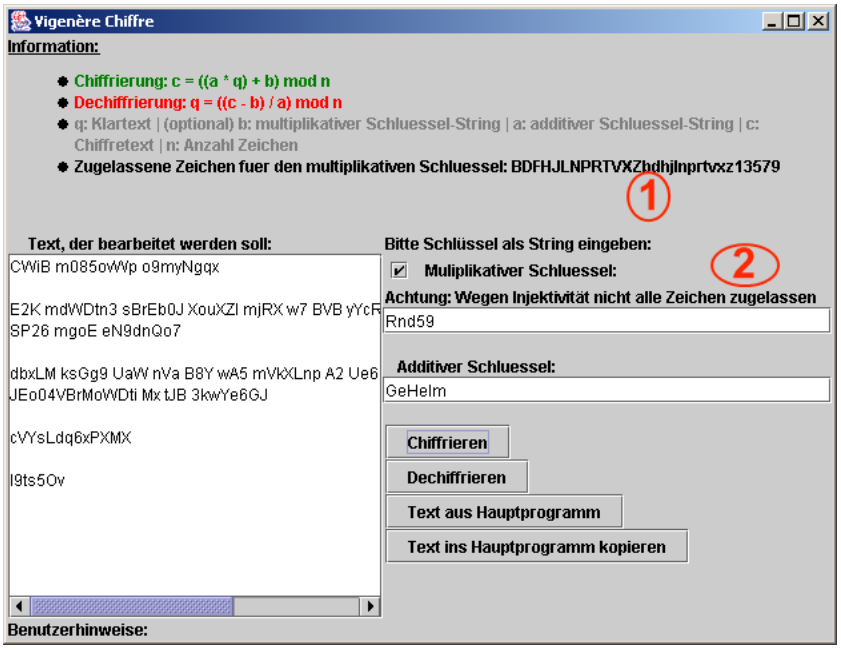

Abbildung 4.7. Dialog Vignère-Chiffre

Das Layout der Vignère-Chiffe wurde analog zum Dialog der affinen Chiffren erstellt. Deshalb wird lediglich auf die Besonderheiten dieses Dialogs eingegangen:

1. Bei den Informationen werden zusätzlich noch alle für den multiplikativen Schlüssel zugelassenen Zeichen aufgelistet
2. Der multiplikative Schlüsel ist optional. Bevor er verwendet werden kann, muss das Häkchen aktiviert werden. Standardmäßig ist diese Funktion deaktiviert. Es sind nicht alle Zeichen für die Eingabe zugelassen. Alle zugelassenen Zeichen kann man oben in den Informaionen sehen (1).

Sollte der multiplikative Schlüssel a_0 ... a_{m-1} nicht aktiviert sein, so erfolgt die Chiffrierung und Dechiffrierung mit einer Folge von 'B' = 1 .

4.4.2 Kasiski-Test

Der Kasiski-Test ist neben dem Koinzidenzindex ein Ansatz zur Analyse der Schlüssellänge. Beide Verfahren wurde so implementiert, dass die Teilfolgen am Ende weiterverarbeitet werden können.

Das Fenster des Kasiski-Test sieht wie folgt aus:

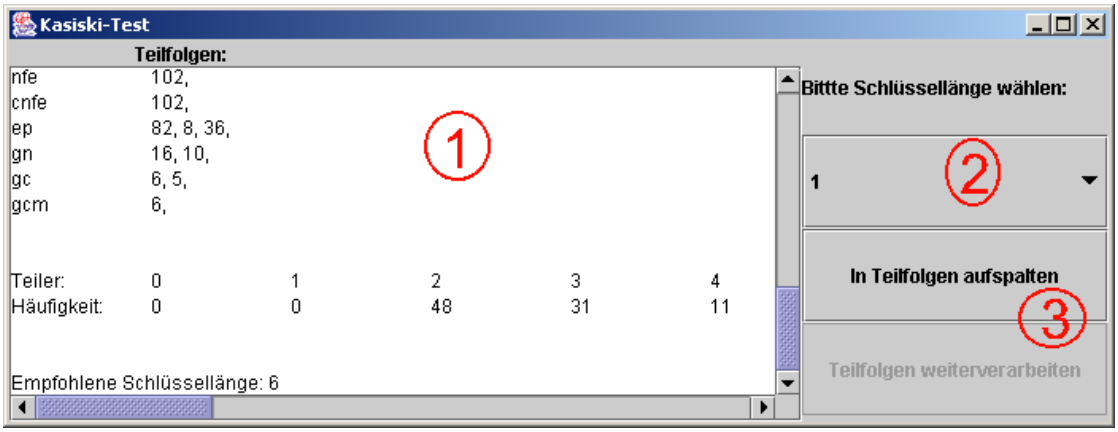

Abbildung 4.8. Dialog Kasiski-Test

Die einzelnen Punkte bedeuten folgendes:

1. Textfeld, das eine häufige Zeichenfolge und deren jeweilige Abstände anzeigt. Darunter werden die Teilerhäufigkeiten und eine Empfehlung für die Teilfolgen angezeigt.
2. Hier kann die Teilfolgen ausgewählt werden. Die Empfehlung für den Blockabstand gibt dem Benutzer eine gute Hilfe bei der Wahl. Die Teilfolge entspricht der Länge des Schlüssels.
3. Nachdem die Blocklänge ausgewählt wurde, kann der Text mit dem entsprechenden Button in Teilfolgen gespaltet werden. Die Teilfolgen werden in dem Textfeld (1) ausgegeben. Nach dieser Aktion kann der Text auch weiterverarbeitet werden.

4.4.3 Koinzidenzindex berechnen

Die Berechnung des Koinzidenzindex ermöglicht eine Analyse der Schlüssellänge. Am Ende können die Teilfolgen weiterverarbeitet werden. Das Fenster zur Berechnung des Koinzidenzindex ist ähnlich aufgebaut (siehe Bild 5.9):

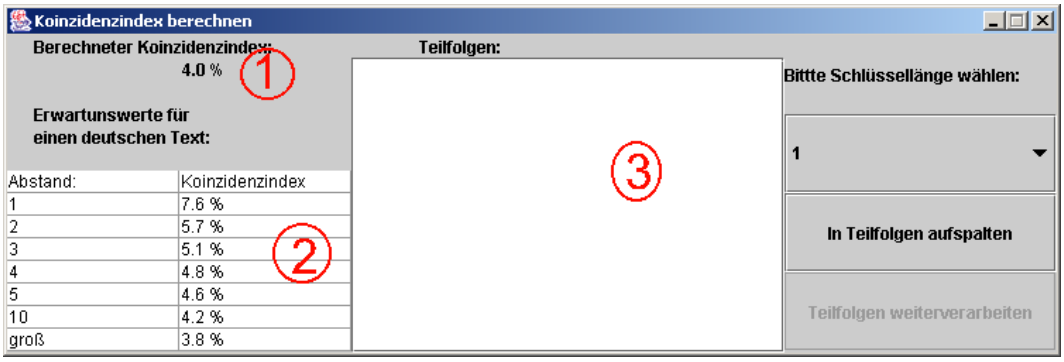

Abbildung 4.9. Dialog Koinzidenzindex-Berechnung

Die einzelnen Punkte bedeuten folgendes:

1. Anzeige des Koinzidenzindex vom Text aus dem Hauptfenster
2. Tabelle mit Koinzidenzindexwerten und empfohlener Schlüssellänge
3. Textfeld, das den Text aus dem Hauptprogramm in Teilfolgen ausgibt,nachdem der entsprechenden Button gedrückt wurde.

4.4.4 Weiterverarbeitung der Teilfolgen

Wenn eine Teilfolge ausgewählt und der Text gespaltet wurde, aktiviert sich bei beiden Verfahren der Button zum Weiterverarbeiten des Textes. Zur Weiterverarbeitung eignen sich, wie in Kapitel 4.4 beschrieben, additive und affine Dechiffrierungsfunktionen. Wird der Button zum Weiterverarbeiten angeklickt, so öffnet sich folgendes Fenster:

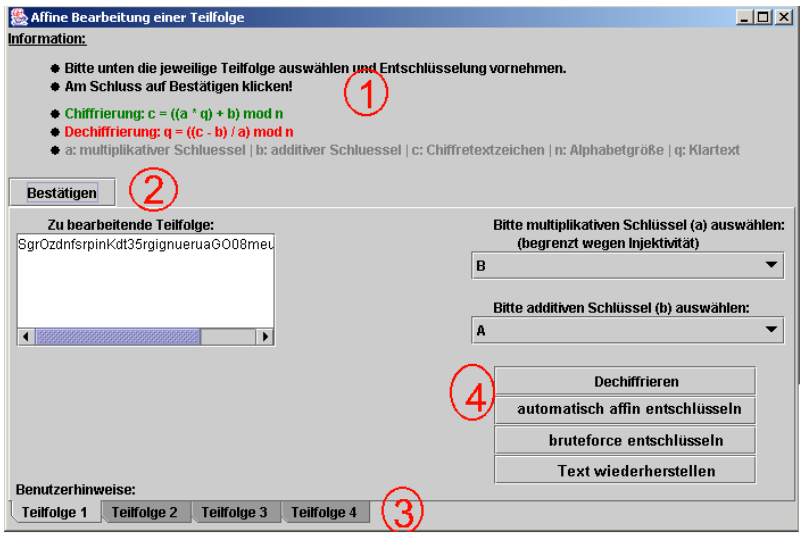

Abbildung 4.10. Dialog Text in Teilfolgen getrennt

In diesem Fenster sind die Texte in die Teilfolgen der jeweiligen Schlüssellänge getrennt (siehe Vorgehen bei polyalphabetischen Chiffren in Kapitel 4.4). Somit sind alle Zeichen, die mit demselben Schlüssel chiffriert werden, zusammen.

Erklärung der Marken:

1. Informationen
2. Button zum Bestätigen, wenn die Bearbeitung der Texte durchgeführt wurde. Dieser öffnet ein Fenster, wo der Gesamtschlüssel angezeigt und der Text wieder zusammengesetzt wird.
3. Auswahl der Blöcke. Wie oben beschrieben ist der ganze Text in einzelne Text mit einer bestimmten Teilfolgen getrennt worden. Hier können jetzt diese einzelnen Texte ausgewählt und bearbeitet werden.
4. Buttons zum Dechiffrieren anhand der ausgewählten Schlüssel, Hilfe in Form einer automatisch affinen Entschlüsselung und einer *bruteforce*-Entschlüsselung des Textes (siehe Kapitel zur automatischen Entschlüsselung von affinen Chiffre unten). Der Text kann mit dem entsprechenden Button auch wiederherstellt werden.

Hinweis: Bitte darauf achten, dass der Text aus der TextArea ständig weiterentschlüsselt wird. Daher sollte darauf geachtet werden, dass die Taste *Wiederherstellen* betätigt, wenn man merkt, dass der Text falsch ist. Wichtig ist die Betätigung des Buttons *Dechiffrieren*, da nur derjenige Text später weitergegeben wird, der in der TextArea steht.

Wenn die Bearbeitung erfolgte und der Button zur Bestätigung gedrückt wurde, öffnet sich folgendes Fenster:

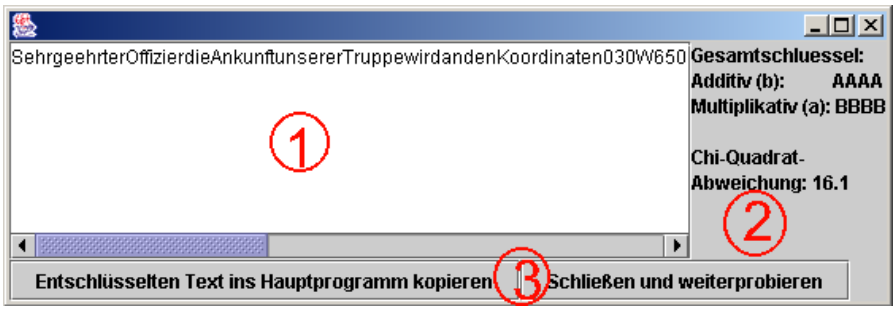

Abbildung 4.11. Dialog Resultat der Aufspaltung in Teilfolgen

Erklärung der Marken:

1. entschlüsselter Text
2. multiplikativen und additiven Gesamtschlüssel sowie der Chi-Quadrat-Wert des Textes
3. Buttons, um den Text ins Hauptprogramm zu kopieren und weiterzuprobieren. Wird der Button zum weiterprobieren gedrückt, so schließt sich das aktuelle Fenster.

4.4.5 Automatische Entschlüsselung

Diese Kategorie umfasst folgende Aktionen:

- Automatisch additiv entschlüsseln
- Automatisch affin entschlüsseln

Über den entsprechenden Menüeintrag gelangen Sie in das jeweilige Fenster. Der Algorithmus zur Entschlüsselung von additiven Chiffre ist recht einfach. Dabei versucht er den Schlüssel als die Differenz zwischen den drei häufigsten Zeichen des Textes und dem häufigsten der deutschen Sprache zu identifizieren. Der Vorgang geht dementsprechend zügig. Es werden alle drei Varianten angezeigt. Das Fenster sieht folgendermaßen aus:

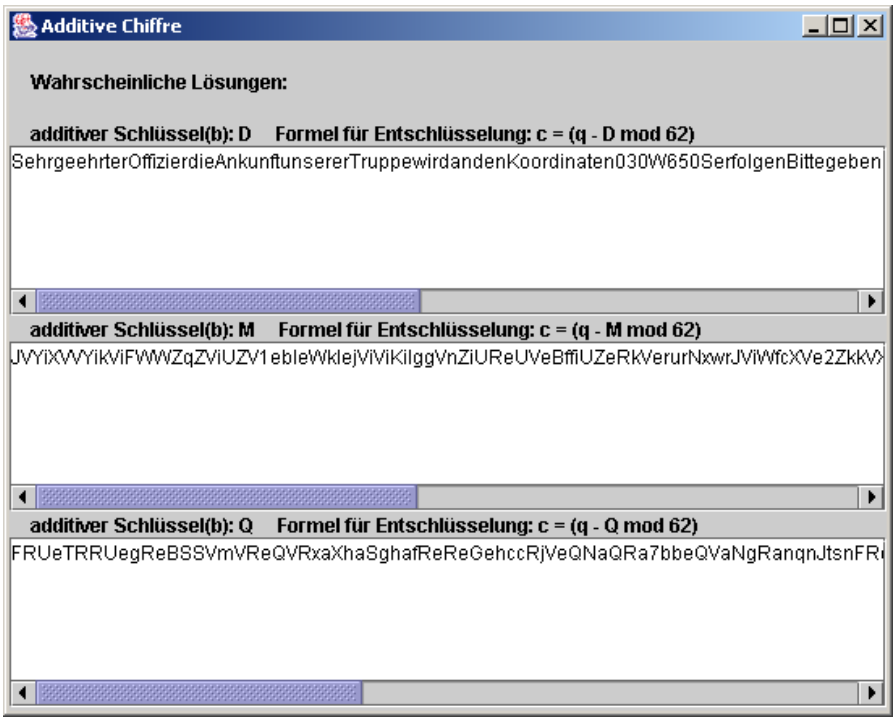

Abbildung 4.12. Dialog automatisch additiv entschlüsseln

Der Algorithmus zur Entschlüsselung der affinen Chiffre ist hingegen komplizierter. Dabei spielt die Chiquadrat-Abweichung zur deutschen Sprache eine sehr wichtige Rolle. Das Programm wurde so eingestellt, dass alle Zeichen bis zu einer Abweichung von 30 Prozent angezeigt werden sollen. Gerade bei großen Alphabeten mit den Klein-, Grossbuchstaben und Zahlen enstehen sehr viele Kombinationsmöglichkeiten, die dann auch jeweils eine recht kleine Abweichung besitzen. Daher dauert der Vorgang bei einem großen Alphabet lange und bietet eben auch viele Resultate. Der Benutzer sollte die Ergebnisse analysieren und die richtige Lösung aussuchen. Das Programm kann ihm dazu nur eine Hilfe geben und eher wahrscheinlichere Resultate und deren Schlüssel

ausgeben.

Es sei darauf hingewiesen, dass das richtige Ergebnis nicht immer mit dieser Methode ermittelbar ist. Daher kann es vorkommen, dass die Ausgabe nur sinnlosen Text liefert. Dieser Fall tritt oft bei kurzen Texten auf.

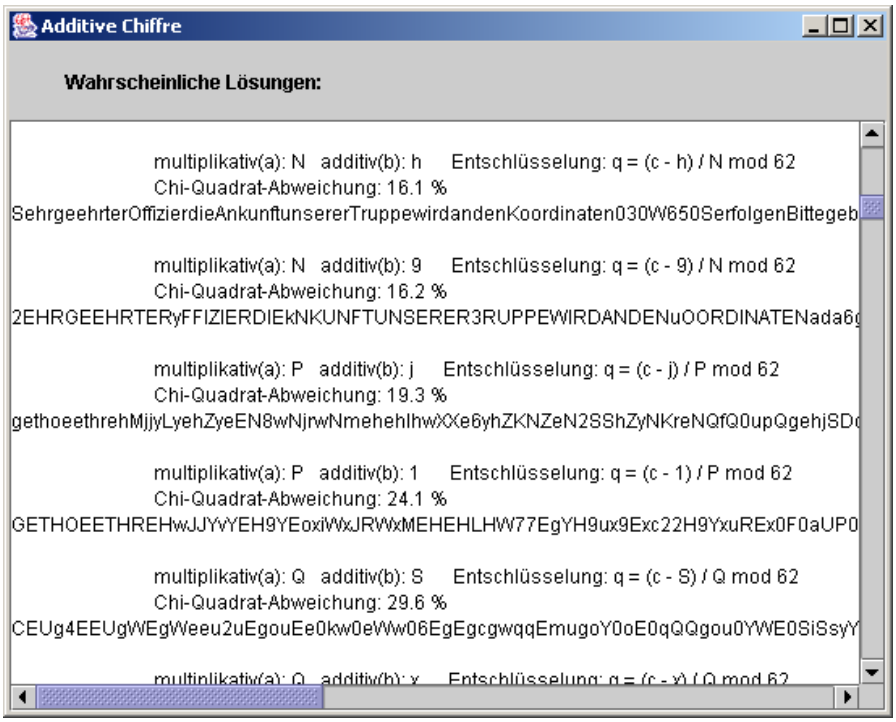

Abbildung 4.13. Dialog automatisch affin entschlüsseln

5

Referenzen

5.1 Literatur

[KryptoSkript:1] *Unterlagen zur Vorlesung Kryptographie WS05/06*
Erschienen: 2005 von Prof. Dr. Alfred Scheerhorn

[KryptoBuch:1] *Kryptographie - Entwurf und Analyse symmetrischer Kryptosysteme*
Erschienen 1988 von W. Funny / H.P. Rieß

5.2 Links

[JavaSDK:1] *Downloadseite für das Java Runtime Environment*

http://java.sun.com/j2se/1.5.0/