Kryptologie

Einführung am Beispiel der mono- und polyalphabetischen Chiffrierungen

Mathias Weigert

Miro Ljubicic

Kurs „Softwareprojekt 2“

Frühlingssemester 2012

Zürcher Hochschule für Angewandte Wissenschaften

School of Engineering

Lagerstrasse 41

8004 Zürich

15. März 2012

aktualisierte Version vom 3. April 2012

# Inhaltsverzeichnis

# Einleitung

## Motivation

Wir interessieren uns beide stark für das Thema Kryptologie und hatten bis jetzt keine Möglichkeit, uns auf diesem Gebiet sinnvoll zu vertiefen.

Da wir momentan für das Hauptstudium hin zu den Themen „Informationssicherheit und Kryptografie“ und „Netzwerktechnik“ tendieren, möchten wir die Chance nutzen, uns schon im Vorfeld intensiv mit den Grundlagen der Informationssicherheit zu befassen.

Der Einstieg in die Grundlagen der Kryptologie und deren Anwendung auf ein fundamentale Fallbeispiele erachten wir als gute Basis.

## Typographische Konventionen

Um die Lesbarkeit des Textes zu erhöhen, werden folgende Konventionen verwendet:

dies ist der klartext Klartext Courier New, klein

ERTS SDF ORT ZIFGHOIP Chiffrierter Text Courier New, gross

Mathematische Formeln Cambria Math, kursiv

# Theorethische Grundlagen

## Monoalphabetische Chiffrierung

### Erkennung monoalphabetischer Chiffrierungen

TO COME (stat. Häufigkeitsverteilung)

### Caesar-Chiffre (Verschiebe-Chiffre)

Der Caesar-Chiffre ist eines der ältesten Verschlüsslungsverfahren. Es zeichnet sich dadurch aus, das man ein Buchstabe des Alphabetes als Schlüssel nimmt und das Alphabet dann um X Stellen verschiebt.

Dieser Chiffre ist extrem einfach und ohne grossen Aufwand zu entschlüsseln. Da nur 26 Schlüssel existieren (Anzahl der Buchstaben im Alphabet).

Beispiel

yippie ya yeah schweinebacke (anderer Text bitte :-)

KUBBUQ KM KQMT EOTIQUZQNMOWQ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 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 |

Der maximale Anzahl von Versuchen um den Caesar-Chiffre zu entschlüsseln beträgt 25 (entspricht der Anzahl Verschiebungen).

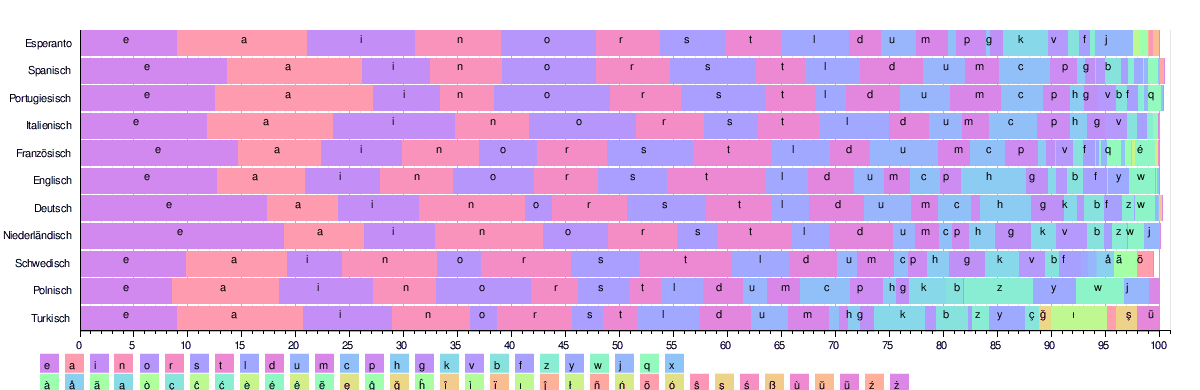
Umsetzung im Programm  
Für die Verschlüsslung mit dem Caesar-Chiffre haben wir folgenden Algorithmus verwendet.

Wobei z das zu verschlüsselnde Zeichen, aus einem Alphabet von 0 bis n-1, ist und k der Wert des Schlüssels.

Zum Dechiffrieren verwenden wir Bruteforce, was bei einer maximalen Schlüsselmenge von 26 und einem Alphabet mit 26 Zeichen am meisten Sinn macht. Die durchschnittliche Dauer bei unserer Implementierung ist ca. 10 ms

### Substitutions-Chiffre

Der Substitution-Chiffre ist schon etwas komplexer da hierbei das Chiffre-Alphabet nicht mehr einfach verschoben wird, sondern völlig willkürlich neu angeordnet wird. Dadurch entsehen 26! Möglichkeiten (das sind 403‘291‘461‘126‘605‘635‘584‘000‘000). Diese Vielzahl der Möglichkeiten würden bei einem simplen Brutforce Algorithmus auch die Heutigen Hochleistungsrechner vor gewisse Probleme stellen. Die Schwachstelle dieses Chiffre liegt in der je nach Sprache ungleich verteilten Buchstaben.



Quelle?

### Kryptoanalyse und Schwachstellen

Statistische Häufigkeitsanalyse  
Gegenbeispiele (Georges Perec – „La Disparition“)

REST TO COME

## Polyalphabetische Chiffrierung

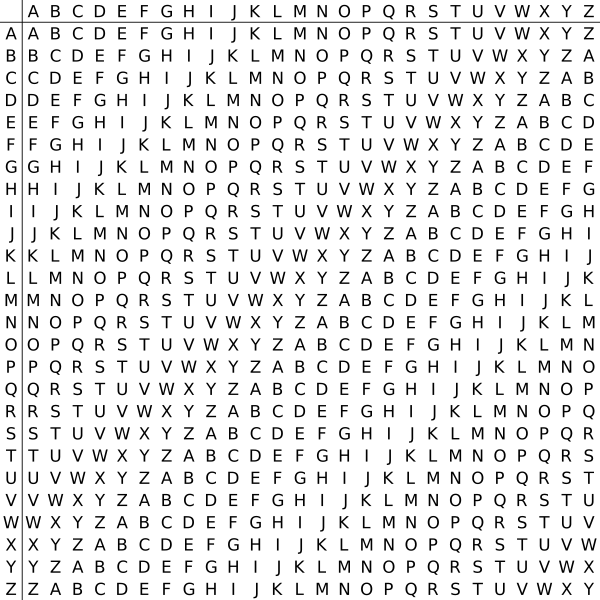
Im Gegensatz zur monoalphabetischen Chiffrierung – welche wie gezeigt

### Vigenère-Chiffre

Das Vigenère-System ist das wohl bekannteste Beispiel der polyalphabetischen Chiffrierungen.  
Die Schlüssel in diesem System sind Texte über dem lateinischen Alphabet.  
Für die Ver- und Entschlüsselung wird das sogenannte „Vignenère-Quadrat“ und ein Codewort definiert.

Jedes einzelne Zeichen des Codeworts beschreibt hierbei die Zeile im Vignenère-Quadrat, welche für die Substitution verwendet werden soll. Nachdem der Klartext nacheinander alle durch das Codewort definierten Substitutionszyklen durchlaufen hat, ist der chiffrierte Text fertig.  
Der chiffrierte Text kann durch Umkehrung des Codeworts auf die gleiche Art in den ursprünglichen Klartext umgewandelt werden.

Dieses Verfahren ist um ein Vielfaches sicherer als monoalphabetische Chiffrierungen, da sich die Anzahl möglicher Schlüssel exponentiell erhöht.  
Sie beträgt beim Vigenère-Code

  
Vigenère-Quadrat (Quelle: <http://de.wikipedia.org/w/index.php?title=Datei:Vigenère_square.svg>)

### Kryptoanalyse und Schwachstellen Euklidische Algorithmus

### Homophone Kryptosysteme

# Implementierung

JAVA CODE HIER

Danksagung (erst zum Schluss)

# Literaturverzeichnis

* Kryptologie – Algebraische Methoden und Algorithmen

(Christian Karpfinger ¦ Hubert Kiechle)

* Deutsche Wikipediaseite (Buchstabenhäufigkeit)

<http://de.wikipedia.org/wiki/Buchstabenh%C3%A4ufigkeit>

* Angewandte Kryptographie

(Wolfgang Ertel)

* The Code Book – The Secret History of Codes and Code-Breaking

(Simon Singh)

* Einführung in die Kryptologie

(Karin Freiermuth ¦ Juraj Hromkovič ¦ Lucia Keller ¦ Björn Steffen)