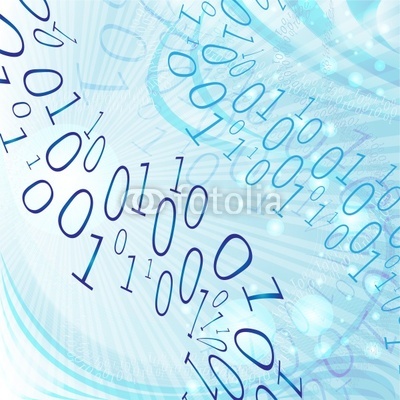
Kryptologie



# Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich ausschließlich auf die Geheimhaltung des Schlüssels.

Kerckhoffs’ Prinzip

# Zürcher Hochschule für angewandte Wissenschaften

## FS2012 – Software Projekt 2

## Gruppe 10 – Miro Ljubicic & Mathias Weigert

# Inhaltsverzeichnis

# Theoretische Grundlagen

Um Irritationen zu vermeiden erst einmal eine wichtige Definition. Wir werden in diesem Skript und auch im Programm immer wieder auf verschlüsselte Texte/Wörter zurück greifen müssen und auch auf die unverschlüsselte Bedeutung. Da es sich allgemein durchgesetzt hat, werden wir ebenfalls den unverschlüsselten Text immer klein schreiben und den chiffrierten Text immer gross.

**Beispiel**

grundlagen

QBEXNVKQOX

### Monoalphabetische Chiffrierung

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

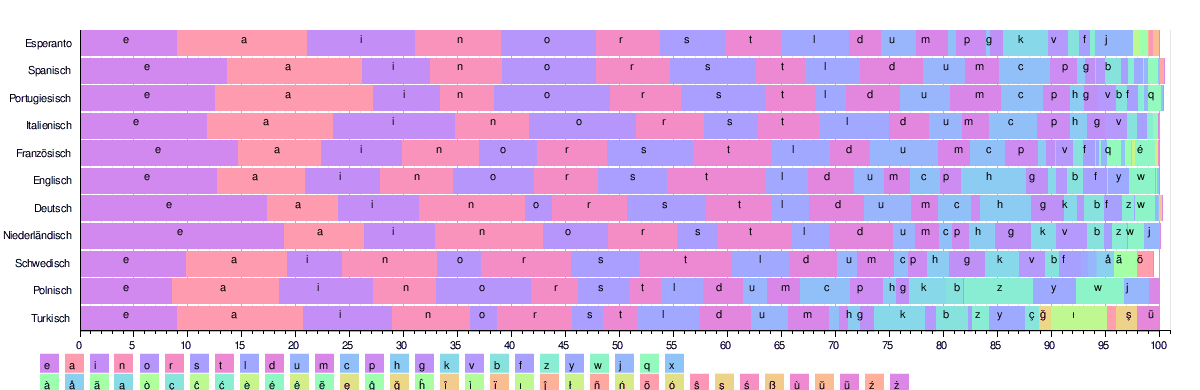
KUBBUQ KM KQMT EOTIQUZQNMOWQ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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.

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.



### Polyalphabetische Chiffrierung

Vigenère-Chiffre

# Umsetzung im Programm

Caesar-Chiffre

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

Wobei das zu verschlüsselnde Zeichen, aus einem Alphabet von bis , ist und der Wert des Schlüssels.

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

# Quellenangabe

* 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)