EIGENES VERSCHLÜSSELUNGSVERFAHREN

Niklas von Hirschfeld

Gymnasium Lüneburger Heide

Grundidee Caeserverfahren

Die Grundidee des **Caeserverfahren** ist die **feste** verschiebung der Buchstaben im Alphabet. Das Vigenere-Verfahren versucht dies durch eine ebenfalls **feste** abfolge von *Schlüsseln* zu erweitern.

Um das Caeserverfahren zu verbessern kann man den Schlüssel dynamischer gestalten. Dafür kann man zum Beispiel:

- Das Schlüsselwort abwechselnd vorwärts und rückwärts anwenden.
- Jeden *Schlüssel* mit dem Vorheriegen verrechnen (z.B. addieren).
- den Schlüssel basierend auf dem Text *generieren*
- Die Schlüssellänge dynamisch gestalten

Man kann auch verschiedene Verfahren auf einander *schichten*. Zum Beispiel in dem man:

- mehrere Schlüssel nacheinander anwenden.
- einmal vorwärst und einmal rückwärts verschlüsselt.
- den selben Schlüssel mehrmals und jeweils versetzt anwenden.
- oder alles zusammen.

Dynamisch Textbasiert

Ich habe mich entschieden den Schlüssel dynamisch, basierend auf dem Text, zu *generieren*. Dafür gibt es ebenfalls verschiedene Ansätze. Man kann zum Beispiel die bis her verschlüsselten Buchstaben mit verrechnen, oder alle noch übrigen Buchstaben.

Mein Ansatzt ist es, die Anzahl der noch im zu verschlüsselnden Text auftauchenden Buchstaben mit zu verwenden und diese mit einem Schlüsselwort zu verknüpfen. Dadurch kann sich der Schlüssel nach jedem entschlüsselten Buchstaben verändern.

Funktionsweise

Beim entschlüsseln mit dem Schlüsselwort „KEY“ werden zunächst alle K's gezählt. Die anzahl dieser wird mit 11 (Position von K im alphabet) addiert. Der erste Buchstabe wird also um so viele Stellen verschoben. Sollte sich dabei die Anzahl der K's im restlichen Text verändern, verändert sich auch der Schlüssel. Abgesehen davon wird wie bei dem Vigenere-Verfahren fortgefahren.

Das Verschlüsseln muss **rückwärts** geschehen, da die bereits verschlüsselten Buchstaben eine Rolle für den Schlüssel spielen. Man fängt also mit dem letzten Buchstaben an verschlüsselt diesen. Sollte der nun codierte Buchstabe in dem Schlüsselwort vorhanden sein, wird die Verschiebung für diesen angepasst.

Sicherheit

Die größte Schwierigkeit beim lösen des Codes ist die Länge des Schlüssels. Bei dem Vigenere-Verfahren kann diese durch sich wiederholende Sequenzen im Text annäherungsweise ermittelt werden. Dies ist hier nicht möglich. Auch hat eine **Häufigkeitsanalyse** eine geringe erfolgswahrscheinlichkeit da auch hier erst die Schlüssellänge benötigt wird.

Nachteile

Unter bestimmten bedingungen kann es durchaus vorkommen, dass diese Verfahren *identisch zum Vigenere-Verfahren* funktioniert. Zum Beispiel, wenn in dem verschlüsselten Text kein einzieges mal ein Buchstabe aus dem Schlüsselwort auftaucht.

Auch ist diese Methode bei **kürzeren** Texten nicht sehr effektiv.