VIGENÈRE-VERFAHREN

Niklas von Hirschfeld

Gymnasium Lüneburger Heide

Einleitung

Das **Vigenère-Verfahren** ist ein *symmetrisches*[1] Verschlüsselungsverfahren, das im 16. Jahrhundert von Blaise de Vigenère entwickelt wurde. Es gilt als eine Weiterentwicklung der einfachen Caesar-Verschlüsselung und wurde über Jahrhunderte als eine der sichersten Methoden zur Verschlüsselung von Texten angesehen. Anders als beim Caesar-Code wird hier ein **Schlüsselwort** verwendet, um den Text zu verschlüsseln.

Funktionsweise

Das Vigenère-Verfahren nutzt eine Reihe von Caesar-Verschiebungen, die durch das Schlüsselwort bestimmt werden. Jeder Buchstabe des Klartextes wird mit einem Buchstaben aus dem Schlüsselwort kombiniert, um einen verschlüsselten Buchstaben zu erzeugen.

Beispiel:

- Klartext: ATTACKE
- Schlüssel: LEMONLE
- Verschlüsselt: LXFOPVE

Hier wird jeder Buchstabe des Klartextes entsprechend dem Buchstaben des Schlüssels verschoben.

Vorteile

Ein großer Vorteil des Vigenère-Verfahrens gegenüber der einfachen Caesar-Verschlüsselung ist die erhöhte **Sicherheit**. Durch die Verwendung eines mehrstelligen Schlüssels wird eine Häufigkeitsanalyse deutlich erschwert, da gleiche Buchstaben im Klartext unterschiedlich verschlüsselt werden können. Dies führte dazu, dass das Verfahren lange Zeit als „unbrechbar“ galt.

[1] Es wird sowohl für die Ver- wie auch Entschlüsselung derselbe Schlüssel verwendet.

Ein weiterer Vorteil ist die **Flexibilität**: Das Verfahren kann leicht angepasst werden, indem man das Schlüsselwort ändert, was eine Vielzahl von möglichen Verschlüsselungen ermöglicht.

Sicherheit

Das Vigenère-Verfahren galt bis ins 19. Jahrhundert als sicher, bis Charles Babbage und später Friedrich Kasiski Methoden entwickelten, um die Verschlüsselung zu brechen. Das Verfahren ist besonders anfällig für die **Kasiski-Untersuchung** und die **Häufigkeitsanalyse** über die wiederkehrenden Buchstabenmuster im Schlüssel.

In der modernen Kryptographie wird das Vigenère-Verfahren als **unsicher** eingestuft, da es durch fortgeschrittene Methoden leicht gebrochen werden kann. Dennoch ist es historisch wichtig, da es den Weg für komplexere Verschlüsselungstechniken ebnete.

Die **Häufigkeitsanalyse** funktioniert hier ähnlich wie bei dem Caeser-Verfahren. Es wird auch hier der am häufigsten auftauchende Buchstabe mit dem in der Sprache generell verglichen. Allerdings muss man hier aufpassen, da die gleichen Buchstaben mit verschiedenen Schlüsseln verschlüsselt sein könne. Nicht jedes *e* ist mit dem selben Schlüssel verschlüsselt. Um die Häufigkeitsanalyse trozdem effektiv anwenden zu könne, ist es von vorteil, wenn die **Schlüssellänge** bekannt ist. Wenn diese zum Beispiel 7 beträgt, wissen wir, dass jedes 7. Wort den selben Schlüssel besitzt. Damit können wir die Häufigkeitsanalyse auf die gruppierten Buchstaben anwenden.

Wenn die Schlüssellänge nicht bekannt ist, kann die **Kasiski-Untersuchung** angewendet werden. Diese hat das Zeil, die länge des Schlüssels herrauszufinden. Dabei werden wiederholte Sequenzen von Buchstaben in dem codierten Text ermittelt und der Abstand dieser analysiert. So kann man annäherungsweise an vielfaches des Schlüssels herausfinden.