

Kryptoanalyse beim Vigenère-Verfahren

Sie haben bereits mithilfe von Häufigkeitsanalysen monoalphabetische Verschlüsselungen geknackt. Dies ist nur dann möglich, wenn statistische Auffälligkeiten des Klartextes auch im Geheimtext wiederzufinden sind. Polyalphabetische Verfahren versuchen daher, statistische Auffälligkeiten des Klartextes beim Verschlüsseln zu „verwischen“:

In der Kryptologie spricht man von **KONFUSION**, wenn sich statistische Auffälligkeiten des Klartextes nicht auf den Geheimtext übertragen.

Aufgaben:

- Geben Sie zwei verschiedene Beispiele für statistische Auffälligkeiten eines Alltagstextes in deutscher Sprache an.
- Erläutern Sie kurz den Unterschied von statistischen Auffälligkeiten von Alltagstexten zu solchen von Fachtexten.
- Beurteilen Sie, inwieweit das Vigenère-Verfahren für Konfusion sorgt.

Die Rolle der Schlüssellänge bei der Kryptoanalyse

Versuchen Sie einmal, den folgenden, mithilfe des Vigenère-Verfahrens verschlüsselten Geheimtext zu knacken. Als Zusatzinformation dürfen Sie davon ausgehen, dass das Schlüsselwort aus drei Buchstaben besteht:

FSEIHDVBWPSIZWEZBDDHUZFMDUVISIZJVMGTCZLZGJZZLIUMZFJXVCPSJNSCOSEBSYZWDOSOORZZR
ZBXZRVNGTCZLZGJZZNJFKZGJJWJOSZISBMMGOCRIOCTGVZWEZGYDBIZWTCSEYZRIUVIHVSHVNURINC
ZWTCHDJSXGWTCWJORRNGTCZLZGJZZNJFKWSZNDZZJRSZNSUMSZWITCGKVPVIZRIUJJHVDZKHOEYS
EBSYZWDOSOOWEYFVDYFGCEISEYWV

Vielleicht hilft Ihnen beim Knacken des Geheimtextes das Programm

HaeufigkeitsanalyseVigenere.xml:

- Importieren Sie die Datei in Snap! und führen Sie das Programm einmal aus. Beschreiben Sie kurz in eigenen Worten die Funktionalität des Algorithmus.
- Versuchen Sie anschließend, mithilfe des Programms das Schlüsselwort für den Geheimtext zu erraten und den Text zu entschlüsseln.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Von der Lizenz ausgenommen ist das InfSII-Logo.

