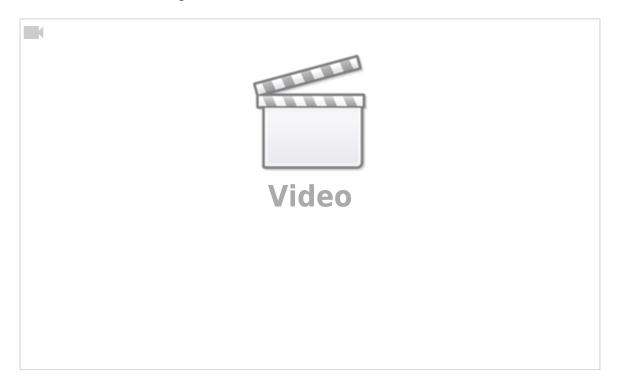
Weiterentwicklung des Substitutionsverfahrens: Vigenère-Chiffre

Durch Häufigkeitsanalysen sind monoalphabetische Substitutionsverfahren unsicher, selbst wenn das Geheimtextalphabet nicht nur verschoben, sondern "zerwürfelt" ist - wenn also die Buchstaben des Geheimtextalphabets in zufälliger Reihenfolge vorliegen. Angriffe auf monoalphabetische Substitutionsverfahren erfolgen immer nach der **Exhaustionsmethode**; sie werden auch als **Brute-Force-Attacken** bezeichnet.

Die Weiterentwicklung der Substitutionsverfahren, die Angriffe auf den Code durch Häufigkeitsanalysen unmöglich macht, ist die **polyalphabetische Substitution** wie wie die Vigenère-Chiffre, die 300 Jahre lang als unangreifbar galt. Hier verwendet man für aufeinanderfolgende Buchstaben jeweils verschiedene Alphabete, so dass sich die Häufigkeiten der Buchstaben im Geheimtext ausgleichen:



Arbeitshilfe: Vigenere-Quadrat

Verwende die

Arbeitshilfen zur Vigenère-Chiffre

und bearbeite folgende Aufgaben.





Aufgaben

- 1. Erkläre das Prinzip von Brute-Force-Attacken (Recherche!).
- 2. Vereinbare mit deinem Nachbarn ein Schlüsselwort. Jeder chiffriert einen kurzen Text (wenige Wörter), ihr tauscht die Geheimtexte aus und jeder dechiffriert die Nachricht des anderen.

Angriff auf die Vigenère-Chiffre: Der Kasiski-Test



Recherchiere Angriffsverfahren auf polyalphabetische Substitutionsverfahren. Stelle einen Angriff, der auf dem **Kasiski-Test** beruht, schematisch (Flussdiagramm) dar.



(A2)

Gegeben ist das folgende Textfragment, welches mit der Vigenere Methode verschlüsselt ist. Es ist bekannt, dass die Schlüssellänge 3 ist.

VRUJEGXEAVNGVBXEDXISILR



(A3)

From:

https://wiki.gg-moessingen.de/ - QG Wiki

Permanent link:

https://wiki.qg-moessingen.de/faecher:informatik:oberstufe:kryptographie:vigenere:start?rev=164553914

Last update: 22.02.2022 15:12

