# Vigenère – polyalphabetische Verfahren

Der Angriffspunkt alle Verfahren, die nur ein Geheimtextalphabet verwenden, ist die Häufigkeit des Auftretens bestimmter Buchstaben und Buchstabengruppen. Der französischer Diplomat Blaise de Vigenère (\* 1523; † 1596) entwickelte auf der Grundlage der Idee des deutschen Benediktinerabt Johannes Trithemius (\* 1462; † 1516) ein Verfahren, das einem Klartextbuchstaben verschiedene Geheimtextbuchstaben zuordnet. Dazu benötigen wir für einen Buchstaben des Schlüsselworts eine eigene Caesar-Scheibe (oder müssen die eine Scheibe immer wieder verstellen).

**Beispiel**

**Schlüssel UNI 🡪 drei Caesar-Scheiben mit den Schlüsseln U, N und I**

Schlüssel: UNIUNIUNI

Klartext: SUEDSTADT

Geheimtext: MHMXFBUQB

Jeder Klartextbuchstabe wird mit der Caesar-Scheibe verschlüsselt, die der Schlüsselbuchstabe angibt.

1. Prüfe das Beispiel nach.
2. Beschreibe die Auswirkung des Verfahrens auf die Häufigkeit der Buchstaben.
3. Entschlüssle den Text FNVXRANNOOAO mit dem Schlüssel UNI.

## 100 % sicher

1. Der Geheimtext MHOAYU wurde mit dem Vigenère-Verfahren verschlüsselt.
2. Zeige, dass sich sowohl der Klartext SCHULE als auch der Klartext PAUSEN in den Geheimtext überführen lassen.
3. Finde einen weiteren Klartext, der sich aus dem Geheimtext rekonstruieren lässt.
4. Wann ist das Vigenère-Verfahren sicher?

Die Erhöhung der Sicherheit geht mit der Verlängerung und der Einmaligkeit des Schlüssels einher. Hat der Schlüssel eine zufällige Buchstabenreihung, die gleiche Länge wie der Klartext und wird nur einmal benutzt, so entsteht das einzige, mathematisch beweisbar nicht knackbare Verfahren: **One Time Pad**. Der diplomatischen Dienst in der Weimarer Republik, der sog. „Heiße Draht“ zwischen den Regierungen während des kalten Kriegs und Che Guevara benutzten One Time Pads.

## Lösung

1. korrekt
2. Die Häufigkeitsverteilung ändert sich. E ist nicht mehr der häufigste Buchstabe, da er in verschiedene überführt wird.
3. Landestagung
4. a) SCHULE 🡪 Schlüssel: UFHGNQ, PAUSEN 🡪 Schlüssel: XHUIUH

4. b) HOELLE 🡪 Schlüssel: FTKPNQ

1. Länge des Schlüssels = Länge des Klartextes