Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

VIGENÈRE – polyalphabetische Verfahren

Die Häufigkeit des Auftretens bestimmter Buchstaben und Buchstabengruppen wird durch Verschlüsselungsverfahren, die Geheimtextalphabet verwenden (monoalphabetische Verfahren), in den Geheimtext übernommen und kann zum Brechen der Verschlüsselung genutzt werden. Diesen Nachteil erkannt der französischer Diplomat BLAISE DE VIGENÈRE (* 1523; † 1596) und entwickelte auf der Grundlage einer Idee des Benediktinerabts JOHANNES TRITHEMIUS (* 1462; † 1516) ein Verfahren, das einem Klartextbuchstaben verschiedene Geheimtext-buchstaben zuordnet.

Beispiel

Schlüssel UNI → je eine Caesar-Scheibe mit dem Schlüssel U, N und I

Schlüssel:	`UNIUNIUNI`
Klartext:	`SUEDSTADT`
Geheimtext:	`MHMXFBUQA`

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

1) Prüfe das gegebene Beispiel. Zeige, dass der letzte Buchstabe falsch sein muss.
2) Beschreibe die Auswirkung des Verfahrens auf die Häufigkeit der Buchstaben.
3) Entschlüssle den Text `FNVXRANNOOAO` mit dem Schlüssel `UNI`?

Arbeitsauftrag Informatik

Name: **Vorname:** **Klasse:**

100 Prozent sicher

Gibt es ein absolut sicheres Verschlüsselungsverfahren? Selbst das VIGENÈRE-Verfahren wurde (immerhin 300 Jahr später) mithilfe statistischer Methoden 1863 geknackt.

Alle bisher besprochenen Verfahren sind zwar unterschiedlich komplex, können aber mit geringem Aufwand heutzutage gebrochen werden. Solche Verfahren eignen sich also nicht (mehr), um vertrauliche Nachrichten, wie z. B. den Internetverkehr beim Online-Banking zu verschlüsseln.

Daher die Frage: Gibt es überhaupt sichere Verfahren?

4) Führe Versuche mit dem VIGENÈRE-Verfahren für den Text CAESAR1.TXT im Programm Cryptool durch.
   a) Verschlüssle dazu den Text mit unterschiedlichen Schlüsseln und lasse anschließend das Programm die Verschlüsselung automatisch brechen (Analyse ' Symmetrische Verschlüsselung (klassisch) ' Ciphertext only ' VIGENÈRE).
   b) Beschreibe Eigenschaften des Schlüssels, damit Cryptool den Text nicht automatisch entschlüsseln kann.
5) Der Geheimtext `MHOAYU` wurde mit dem VIGENÈRE-Verfahren verschlüsselt.
   c) Zeige, dass sich sowohl der Klartext `SCHULE` als auch der Klartext `PAUSEN` in den Geheimtext überführen lassen.
   d) Finde einen weiteren Klartext, der sich aus dem Geheimtext rekonstruieren lässt.
6) 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 diplomatische Dienst in der Weimarer Republik, der sog. „Heiße Draht“ zwischen den Regierungen während des kalten Kriegs und CHE GUEVARA benutzten One Time Pads.

Für zukünftige (moderne) Verfahren muss gelten: „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Sie gründet sich nur auf die Geheimhaltung des Schlüssels.“

(Prinzip Nr. 2 des Niederländer Kryptologen AUGUSTE KERKHOFFS aus dem Jahre 1885).