# Geheimschriften*.

Schon immer übten Geheimschriften eine gewisse Faszination auf den Menschen aus. Bereits *Julius Caesar* benutzte ein Geheimschriftverfahren. Es gibt verschiedene Methoden, um Texte zu verschlüsseln und wieder zu entschlüsseln [1].

einfache Substitution

Ein Prinzip einer Verschlüsselung besteht darin, jeden Buchstaben aus der gleichen Menge zu ersetzen. Je schwieriger die Ersetzungsregeln sind, desto schwieriger ist die Geheimschrift zu entziffern. Julius Caesar benutzte die einfache Substitutionsregel A –> D, B –> E, C –> F ... Z –> C. Solche Geheimschriften kann man durch Berücksichtigung der Buchstabenhäufigkeit entschlüsseln.

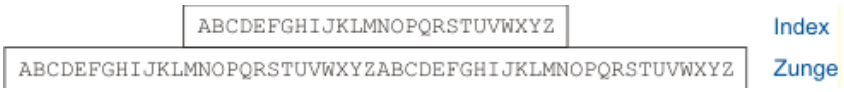
zweifache Substitution

Im Folgenden soll ein Verschlüsselungsverfahren durch Zweifachsubstitution dargestellt werden. Es wird auf *Blaise de Vigenére* und *Tritemius* zurückgeführt. Nach dieser Methode wird aus stets wechselnden Alphabeten zweimal substituiert. Dieses Verschlüsselungsverfahren war rund *300 Jahre lang nicht zu enträtseln*. Erst 1863 veröffentlichte der preußische Infanteriemajor *Friedrich W. Kasiski* ein systematisches Verfahren zur Entschlüsselung.

Verschlüs-selungs-methode:

Zur Verschlüsselung wird ein *Schlüsselwort* benötigt, das die Auswahl der 26 möglichen zyklischen Vertauschungen der alphabetischen Anordnung A, B, C, ... steuert.

Um im jeweils ausgewählten Alphabet das richtige Ersetzungssymbol zu finden, benutzt man den sogenannten *St.-Cyr-Schieber* (nach der gleichnamigen französischen Militärschule, die ihn um 1880 benutzte), dessen zwei Teile gegeneinander verschiebbar sind wie bei einem Rechenschieber (Abb. 1).




Soll der Text CODIERUNGSTHEORIE verschlüsselt werden und lautet das Schlüsselwort INFORMATIK, dann stellt man für jeden Buchstaben des Klartextes zusammengehörige Buchstabenpaare auf Index und Zunge untereinander.

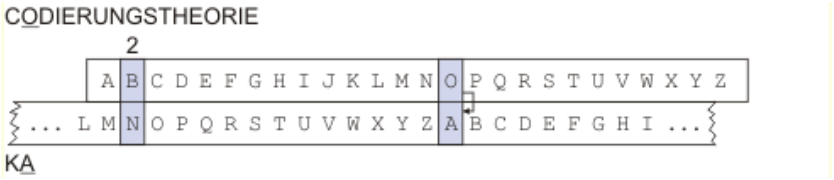
Beispiel

Für den ersten Buchstaben des Klartextes (C) stellt man den ersten Buchstaben des Alphabets (A) auf dem Index über den ersten Buchstaben des Schlüsselworts (I) auf der Zunge ein (Abb. 2).


Dann sucht man auf dem Index den Klartextbuchstaben, auf der Zunge darunter steht dann der Codebuchstabe (K).

Für den nächsten Buchstaben sieht das dann wie in der Abb. 3 und der

Abb. 4aus.

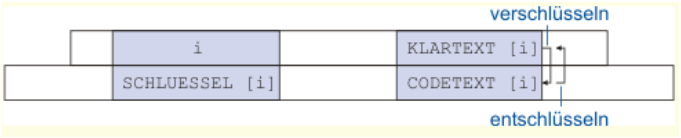




Auf diese Weise erhält man für den Klartext CODIERUNGSTHEORIE den Codetext KAGTRYOZGTRJXPUFO.

Ist der Klartext länger als das Schlüsselwort, dann wird das Schlüsselwort so oft hintereinander gelegt, wie der Klartext es fordert. Ebenso werden die 26 Buchstaben des Alphabets hintereinander gestellt.

Allgemein erhält man das Schema der Abb. 5.




i = laufende Nummer der Buchstabenfolge im Klartext.
SCHLÜSSEL [i], KLARTEXT [i] und CODETEXT [i] sei jeweils der Ordnungswert des i-ten Buchstabens des Schlüsselworts, des Klartextes und des Codetextes.

Es ergibt sich die Gleichung der Abb. 6.

KLARTEXT [ i ] – i = CODETEXT [ i ] – SCHLUESSEL [ i ]

Für das Entschlüsseln gilt die gleiche Anordnung. Zur Decodierung des 1. Codebuchstabens wird der 1. Buchstabe des Alphabets (A) auf dem Index über den ersten Buchstaben des Schlüsselwortes (I) auf der Zunge eingestellt. Dann sucht man auf der Zunge den Codetextbuchstaben, auf dem Index darüber steht der Klartextbuchstabe (C) usw.

Aufgabe:
Entwerfen Sie einen Algorithmus zum Verschlüsseln und Entschlüsseln von Texten nach der erläuterten Methode und realisieren Sie den Algorithmus als Java-Programm. Die Ausgabe soll folgende Form aufweisen:

```
Schlüsselwort:
INFORMATIK
Text:
CODIERUNGSTHEORIE
Verschlüsselter Text:
```

```
KAGTRYOZGTRJXPUFO

Schlüsselwort:
INFORMATIK
Text:
KAGTRYOZGTRJXPUFO
Entschlüsselter Text:
CODIERUNGSTHEORIE
```

Das Programm soll wahlweise entschlüsseln oder verschlüsseln für beliebige Schlüsselworte. Entschlüsseln Sie mit Ihrem Programm folgenden Text (Schlüsselwort: INFORMATIK):

LMVSNIYZSJCCUFUPOJHJQZXVGTEEGJLBRPNVYVZGUQRENGKGZE
SQMGXPAFKQFSMPFSUOWK

Ergänzende Bemerkungen

Es stellt sich jetzt natürlich die Frage, ob man einen Codetext entschlüsseln kann, wenn man das Schlüsselwort nicht kennt. Bazaries hat um 1880 eine Methode erfunden, die auf der Voraussetzung beruht, dass man ein Wort errät, das mit großer Wahrscheinlichkeit im Klartext enthalten ist. Die Idee dabei ist, dass die Beziehung zwischen Schlüsselwort und Klartext umkehrbar ist, d.h. das im Klartext vermutete Wort wird als Schlüsselwort benutzt und der Codetext als Codetext. Dann muss unter dem vermuteten Wort als Klartext bei der Entschlüsselung das wirkliche Schlüsselwort erscheinen, wenn auch evtl. in einer zyklischen Vertauschung der Buchstabenfolge. Da man nicht wissen kann, wo das vermutete Wort im Klartext steht muss die »richtige Stelle« durch systematisches Probieren gefunden werden, bis man das Schlüsselwort erkennt. Diese Methode versagt, wenn das Schlüsselwort eine willkürliche Buchstabenfolge ist. Eine Verallgemeinerung der hier dargestellten Methode liegt vor, wenn das Alphabet auf dem St.-Cyr-Schieber anders angeordnet ist (irrationales Alphabet). Außerdem kann man mit mehreren Alphabeten arbeiten oder das Schlüsselwort nach einer bestimmten Anzahl von Zeichen ändern. Dies ist das Grundprinzip der maschinellen Verschlüsselung.

Zusatz für Liebhaber

Eine ähnliche Verschlüsselungsmethode wird in dem Roman »Und Jimmy ging zum Regenbogen« (Schlüsselwort) von Johannes Mario Simmel (S. 336 ff.) beschrieben. Entwerfen Sie einen Algorithmus für dieses Verfahren.