1.1. Vorteile der Verschlüsselung als Einstieg in die Wahrscheinlichkeitsrechnung

Frieder Roggenstein

In den folgenden Kapiteln wird eine Möglichkeit aufgezeigt das Thema Wahrscheinlichkeitsrechnung einzuführen.

Zuerst erleben die Schüler auf spielerische Art und Weise das Prinzip des Verbergens. Daraufhin lernen sie unterschiedliche Verfahren zur Verschlüsselung von Texten kennen. Anhand der Entschlüsselung durch eine Wahrscheinlichkeitsanalyse wird der Bogen zum Thema Wahrscheinlichkeitsrechnung gespannt.

Hintergründe

Alltagsnähe

Die Verschlüsselung als Einstieg in das Thema Wahrscheinlichkeitsrechnung ist für die Schüler sehr ansprechend, da sie aus ihrem eigenen Leben gegriffen ist. Die meisten Schüler haben schon einmal Nachrichten verschickt, die nicht für jedermanns Augen bestimmt waren. Außerdem werden sie vor allem durch das Internet ständig mit verschlüsselten Inhalten konfrontiert. Die Motivation ist daher besonders hoch und die Schüler nutzen das Erlernte vielleicht sogar außerhalb des Mathematikunterrichts.

Problemorientierter Ansatz

Außerdem weckt der problemorientierte Ansatz, einen Text selbst ent-/verschlüsseln zu müssen, den Ehrgeiz vieler Schüler. Dieser Effekt wird bei einem typischen Einstieg mit einem Glücksspiel, wie zum Beispiel Würfeln oder Lotto nicht erzielt.

Spielerisches Lernen

Aufgrund des spielerischen Charakters des Unterrichts bemerken die Schüler gar nicht, dass sie sich mit Mathematik beschäftigen. Das selbstständige Ausprobieren und Knobeln ermöglicht ein besseres Verständnis des Erlernten.

Kulturelle Bildung

Die Kodierung von Daten ist ein fester Bestandteil unseres Alltags. Schon damals im alten Rom wurde das Prinzip des Verschlüsselns zur Überbringung von geheimen Nachrichten genutzt. Auch im zweiten Weltkrieg spielte die Kodierung mit der bekannten Rotor-Schlüsselmaschine Enigma eine große Rolle. Das Thema bietet sich daher auch für fächerübergreifenden Unterricht an. Die Verschlüsselung wird heute nicht mehr nur von Geheimdiensten und dem Militär angewandt, sondern ist aus dem Zeitalter des Internets nicht mehr wegzudenken. Ein weiterer Grund dafür, dass den Schülern dieses Thema nahegebracht werden sollte.

1.2. Zollspiel

Frieder Roggenstein

Dies ist eine Hinführung zur Wahrscheinlichkeitsrechnung. Es gibt zwei Möglichkeiten Nachrichten geheim zu halten: Das Verbergen und das Verschlüsseln. Das folgende Spiel thematisiert das Verbergen.

Konkrete Umsetzung

Es werden vier Schüler ausgewählt, die in die Rolle von Schmugglern schlüpfen und acht weitere Schüler, deren Aufgabe es ist, als Zollbeamte das Schmuggeln zu verhindern.
Die vier Schmuggler bekommen einen kleinen Gegenstand – zum Beispiel eine SD-Speicherkarte – und gehen damit vor die Türe. Ihre Aufgabe ist es diesen so zu verstecken, dass sie damit an allen Zollbeamten vorbeikommen und die andere Seite des Klassenzimmers erreichen. Wer von ihnen der eigentliche Schmuggler ist und wo er oder sie den Gegenstand versteckt hat, bleibt den Zuschauern und den Zollbeamten verborgen.

Die Zollbeamten stellen sich immer zu zweit gegenüber in einer Reihe auf und dürfen die Schmuggler durchsuchen, wobei natürlich auf deren Intimsphäre Rücksicht genommen werden muss. Jeder Schmuggler muss alle vier Stationen durchlaufen haben, bevor er die andere Seite des Klassenzimmers erreicht. Pro Station haben die Zollbeamten 20 Sekunden Zeit.
Wenn ein Schmuggler auffliegt und der Gegenstand gefunden wird, wird das Spiel abgebrochen.

Erweiterung

Wird der versteckte Gegenstand bis zum Schluss nicht gefunden, kann man das Spiel erweitern, indem man die Verdächtigen in einem Verhör befragt. Vor der Auflösung darf jeder Schüler der Klasse einen Tipp abgeben, wer der Schmuggler ist.

Hintergründe

Spannungs- und Erwartungshaltung

Die Schüler erleben das Prinzip des Verbergens auf eine spielerische Weise. Gleichzeitig ist die Übung sehr alltagsnah, da viele Schüler bereits am Flughafen oder im Fußballstadion eine solche Durchsuchung erlebt haben. Auch das Lesen der Gesichter und das eigene Mitraten, wer denn wohl der Schmuggler sein könnte, sorgt für Spannung und Interesse.

Gemeinsame Grundlage von Verbergen und Verschlüsseln

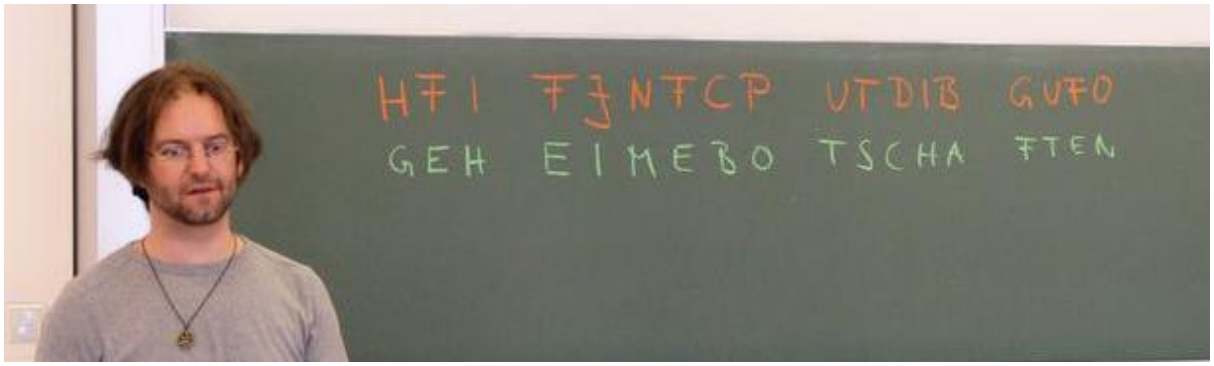
Durch die Veranschaulichung des Verbergens wird den Schülern der Sinn des späteren Themas Verschlüsselung bewusst: In beiden Fällen geht es um die Weitergabe eines Geheimnisses, ohne dass es bekannt wird. Die Verschlüsselung geht einen Schritt weiter und schützt auch vor dem Fall, dass die Nachricht in die falschen Hände gerät.

1.3. Die Caesar-Verschlüsselung

Janik Isele

Mithilfe der einfach zu durchschauenden Caesar-Verschlüsselung werden die Prinzipien der Ver- und Entschlüsselung aufgezeigt.

Konkrete Umsetzung



Die Lehrkraft notiert eine kurze verschlüsselte Botschaft mit roter Kreide an die Tafel. Die Aufforderung an die Klasse lautet nun schlicht:

“Wer herausfindet, was die Botschaft bedeutet, sagt „Eins!“. Die zweite Person, die das Rätsel löst, sagt „Zwei!“ und so weiter. Mal sehen, wie lange es dauert, bis ihr bei 30[1] angekommen seid.“
Der Prozess kann entweder strikt fortgeführt werden, bis die genannte Zahl erreicht wird oder aber früher beschleunigt werden. Hierzu werden diejenigen Schüler, die die Lösung bereits kennen, aufgefordert, den ersten Buchstaben zu nennen. Dieser wird mit grüner Kreide (Klartext) unter den ersten roten Buchstaben (verschlüsselter Text) notiert. Für den Fall, dass der erste alleine nicht weiterhilft, wird auch der zweite Buchstabe aufgelöst. Aufgrund der Einfachheit der Chiffrierung sollte nun auch beim Rest der Klasse der „Aha!-Effekt“ einsetzen. Erkennt kein einziger Schüler die Verschlüsselung, so wird der erste Lösungsbuchstabe durch den Lehrer eingesetzt. Zum Ende der Übung steht die vollständig entschlüsselte Botschaft in grüner Farbe so unter der geheimen Nachricht, dass jeweils ein grüner und ein roter Buchstabe einander zugeordnet werden können. Einer der Schüler erläutert abschließend die Funktionsweise der Caesar-Chiffre. Das folgende Tafelbild dient dabei der Unterstützung.

Auflösung

Die Caesar-Verschlüsselung basiert auf einer Verschiebung des Alphabets. Hierzu wird dieses zunächst in grüner Schrift vollständig in einer Zeile notiert. Anschließend wird mit roter Kreide ein zweites Alphabet darunter geschrieben, nun allerdings zyklisch nach rechts verschoben. In unserem einfachen Beispiel besteht die Verschiebung aus nur einem Schritt, d.h. das neue rote Alphabet beginnt mit dem Buchstaben B. Das A bildet entsprechend das letzte Glied und wird als 26. Buchstabe an das Z angehängt. Die so entstandenen Zeilen sind der Schlüssel, mit dem geheime Botschaften sowohl geschrieben, als auch entziffert werden können. Ersteres geschieht, indem die zu verschlüsselnden Worte (in grüner Farbe) aufgeschrieben werden und anschließend Schritt für Schritt jeder grüne Buchstabe durch den entsprechenden roten ausgetauscht wird. Falls die Art der Chiffrierung bekannt ist, funktioniert die Entschlüsselung dementsprechend in entgegengesetzter Richtung. Bewusst eingebaute Rechtschreibfehler oder falsch bzw. gar nicht gesetzte Leerzeichen erschweren die Entschlüsselung.
Ist die Anzahl der Verschiebungsschritte unbekannt, muss die sogenannte Wahrscheinlichkeitsanalyse angewandt werden (siehe Kapitel 1.4).

[1] Diese Zahl ist (im Rahmen der Klassenstärke) prinzipiell frei wählbar, sollte aber groß genug sein, um herausfordernd zu wirken.

Hintergründe

Verschlüsseln statt Verbergen

Die Caesar-Verschlüsselung, deren Titel auf ihre Verwendung durch den gleichnamigen Feldherrn zurückgeht, schließt an die Thematik des Zollspiels an. Ziel beider Übungen ist es, den Inhalt einer Botschaft geheim zu halten. Während das Verbergen der Nachricht im Zollspiel diese vor den Augen Dritter schützen soll, stellt die reine Sichtung für ein verschlüsseltes Schreiben kein Problem dar. Allerdings sollen Unbefugte in diesem weiteren Schritt der Absicherung nicht mehr in der Lage sein, den Inhalt des Textes zu verstehen. Beide Wege stellen Möglichkeiten der vertraulichen Kommunikation dar, bei der der direkte Kontakt von Angesicht zu Angesicht nicht möglich ist.

Rätselcharakter

Der herausfordernde Charakter der Übung spornt die Schüler an, da sie unter den Ersten sein wollen, die das Rätsel lösen. Ähnlich wie das „Versteckspiel“ der Schmuggler stammt auch dieses „Knobeln“ aus der Lebenswelt der Kinder, wodurch sie einen direkten Bezug zur Aufgabe besitzen.
Neben dem oben genannten Effekt herrscht weiter ein gewisser Gruppendruck, da niemand die Rolle des Unwissenden annehmen möchte. Dadurch wird ein lange anhaltendes, hohes Maß an Motivation sichergestellt, welches ausschließlich von der Art der Aufgabenstellung und nicht von externen Anreizen durch den Lehrer ausgeht.

Einfachheit

Dass diese Art der Caesar-Verschlüsselung vergleichsweise schnell zu durchschauen ist, hat gleich mehrere Vorteile: Zum einen wird dadurch der Einstieg in die Thematik der Chiffrierungen erleichtert und die oben genannte Motivation aufrechterhalten, da unlösbar erscheinende Rätsel zu schnell an Reiz verlieren. Des weiteren werden die Schüler so von selbst auf eine Frage aufmerksam, die sich beim Umgang mit Verschlüsselungen zwangsläufig stellt: Wie lässt sich die Sicherheit der Chiffrierungen erhöhen? Damit wird nicht nur die Neugierde der Schüler geweckt, sondern auch die Überleitung zu ausgefalleneren Verschlüsselungen geschaffen.

1.4. Die Wahrscheinlichkeitsanalyse

Janik Isele

Die Wahrscheinlichkeitsanalyse ist ein Hilfsmittel zur Entschlüsselung komplexerer Kodierungen und Chiffren, beispielsweise der Caesar-Verschlüsselung mit mehreren Verschiebungsschritten.

Konkrete Umsetzung

Die Schüler erhalten ein DinA4-Blatt, auf welchem ein teilweise verschlüsselter Text zu sehen ist. Dabei wurden einige Buchstaben durch Sonderzeichen ersetzt, während die restlichen unverschlüsselt blieben. Ziel ist es nun, den Text mithilfe der Wahrscheinlichkeitsanalyse zu entschlüsseln. Als Hilfsmittel steht den Schülern eine Häufigkeitstabelle zur Verfügung, welche das prozentuale Vorkommen jedes Buchstaben innerhalb der deutschen Sprache beziffert:

DAMITK+I$DRITT+R
DI+BOT@CHAFT7+@+$
KA$$,WIRD@I+
V+R@T+CKTOD+R
V+R@CH7Ü@@+7T.

Platz	Buchstabe	Relative Häufigkeit
1.	E	17,40%
2.	N	9,78%
3.	I	7,55%
4.	S	7,27%
5.	R	7,00%
6.	A	6,51%
7.	T	6,15%
8.	D	5,08%
9.	H	4,76%
10.	U	4,35%
11.	L	3,44%
12.	C	3,06%
13.	G	3,01%
14.	M	2,53%
15.	O	2,51%
16.	B	1,89%
17.	W	1,89%
18.	F	1,66%
19.	K	1,21%
20.	Z	1,13%
21.	P	0,79%
22.	V	0,67%
23.	ß	0,31%
24.	J	0,27%
25.	Y	0,04%
26.	X	0,03%

Erstellen der Textvorlage

Das Erstellen solcher Texte geht mithilfe gängiger Office-Programme wie Microsoft Word oder LibreOffice zügig und leicht von der Hand. Dazu wird zunächst die unverschlüsselte Version eingegeben. Anschließend wird die Suchfunktion aufgerufen

und der Buchstabe eingetippt, der ersetzt werden soll. Darunter lässt sich das gewünschte Sonderzeichen angeben. Klickt man nun die Taste „Ersetze alle“ (LibreOffice) bzw. „Alle ersetzen“ (Word), vertauscht das Programm automatisch den gewöhnlichen Buchstaben und das Sonderzeichen.

Anzahl verschlüsselter Buchstaben

Einen der Knackpunkte dieser Übung stellt die Zahl der Buchstaben dar, die verschlüsselt werden. Wird der Großteil des Textes im ursprünglichen Zustand belassen, so bietet dies den Vorteil, dass sich mögliche Lösungen schnell durch Einsetzen kontrollieren lassen. Findet ein Schüler beispielsweise ein Wort mit lediglich einem Sonderzeichen, so kann er leicht überprüfen, welcher Buchstabe an dieser Stelle Sinn ergibt. Gleichzeitig lässt sich durch diesen Trick jedoch die eigentliche Wahrscheinlichkeitsanalyse durch bloßes Raten umgehen, wenn derartige Worte zu oft auftreten. Es empfiehlt sich also, eine mittlere Anzahl an Buchstaben zu verschlüsseln.

Hintergründe

Bezug zum Bildungsplan

Durch die Verwendung der Häufigkeitsverteilung knüpft diese Aufgabe an den Themenblock der Wahrscheinlichkeitsrechnung an, der im Bildungsplan als Leitidee „Daten und Zufall“ auftritt. Es empfiehlt sich beispielsweise, anhand der Häufigkeitstabelle und dem Vorkommen einzelner Buchstaben im Text die Differenzierung von absoluter und relativer Häufigkeit einzuführen. In diesem Zusammenhang lässt sich auch das Gesetz der großen Zahlen erarbeiten, da sich die relative Häufigkeit eines Buchstaben innerhalb des Textes mit zunehmender Länge des Aufsatzes dem Erwartungswert aus der Tabelle annähert.

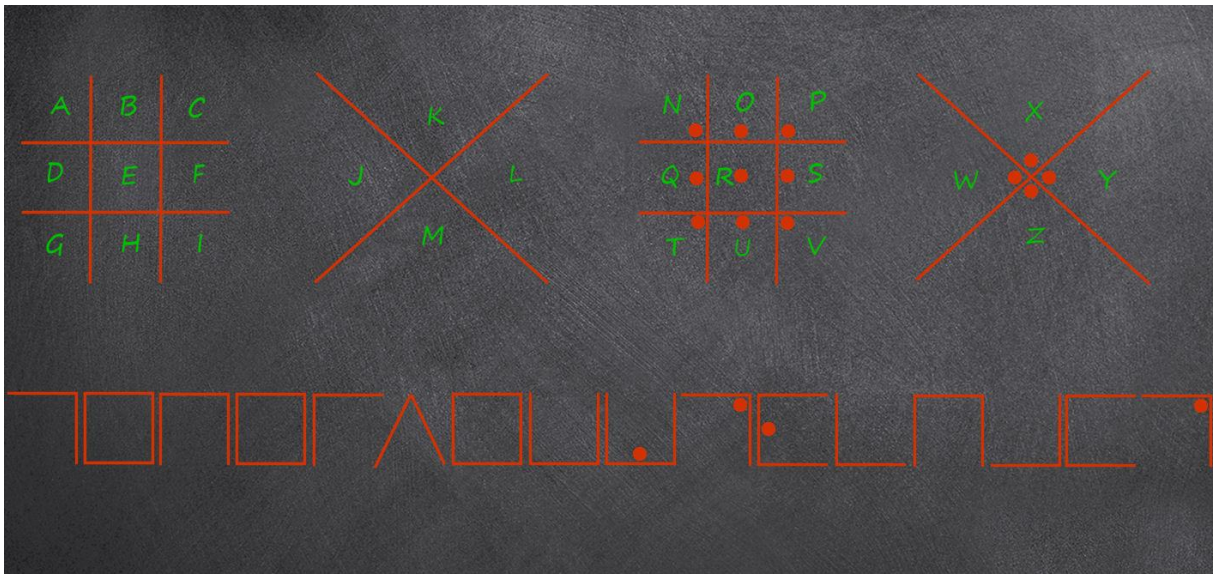
1.5. Der Freimaurercode

Janik Isele

Der aufgrund seiner mystischen Optik besonders ansprechend auf die Schüler wirkende Freimaurercode stellt eine Alternative zur Caesar-Verschlüsselung dar.

Konkrete Umsetzung

Sowohl die geheime Botschaft, als auch die zugehörige Kodierungstabelle werden an der Tafel angebracht. Das restliche Vorgehen verläuft nun analog zur Einführung der Caesar-Verschlüsselung.



Auflösung

Im Unterschied zu Chiffrierungen verwenden Kodierungen keine gewöhnlichen Buchstaben, sondern sonstige Symbole und Zeichen. Der Freimaurercode ersetzt jeden Buchstaben durch die Umrandungslinien die ihn in der Kodierungstabelle umgeben. In der hier verwendeten Version tauchen zusätzlich Punkte auf, die beispielsweise die Unterscheidung der Buchstaben A und N ermöglichen, denen ansonsten das selbe Symbol zugeordnet würde.

Hintergründe

Mystik

Durch die kryptisch wirkenden Zeichen entsteht zusätzlich zur grundsätzlich gegebenen Motivation (die auch bei anderen Verschlüsselungsarten vorhanden ist) der Reiz des Unbekannten. Der Name des Freimaurercodes trägt sein Übriges zu diesem Umstand bei, da den Geheimbund eine Aura des Mystischen umgibt.

Vorgabe der Entschlüsselungsregel

Durch das Vorgeben der Kodierungstabelle unterscheidet sich die Verwendung des Freimaurercodes von dem Vorgehen bei der Caesar-Verschlüsselung, da hier das Herausfinden der Botschaft eher einer Fingerübung als einem Rätsel gleicht. Als weiterführende Übung lässt sich jedoch auch das „Knacken“ des Codes einbinden, indem abgewandelte Kodierungstabellen verwendet werden, die den Schülern nicht vorgegeben werden. Lösbar wird diese Aufgabe durch die Verwendung der Wahrscheinlichkeitsanalyse.

1.6. Die Vigenère-Verschlüsselung

Janik Isele

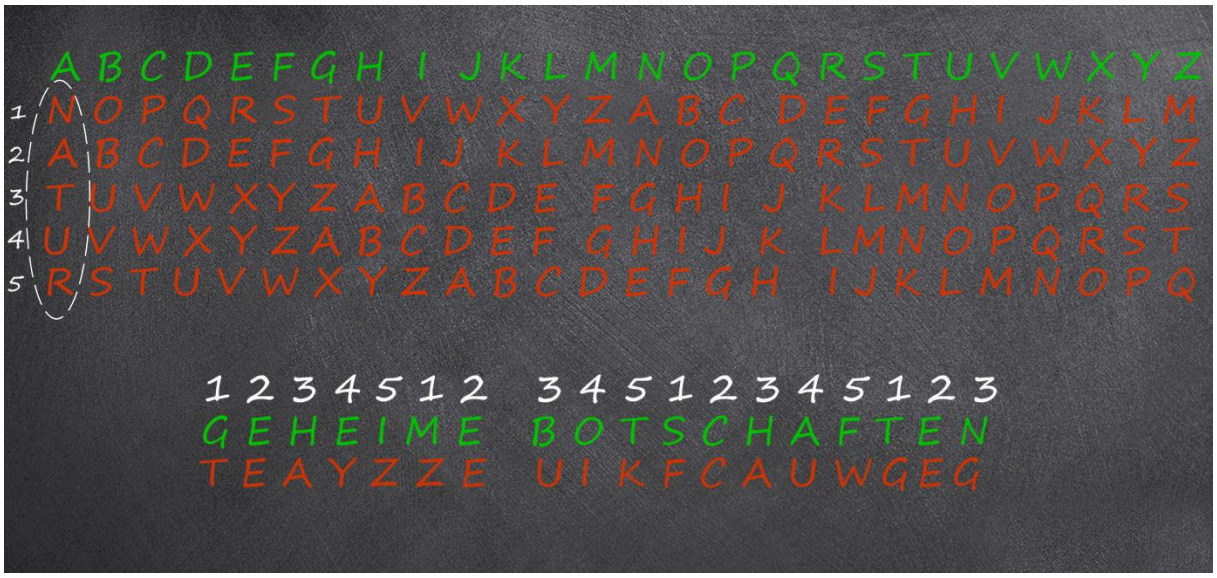
In dieser Übung werden die Schüler erstmals mit einer komplexeren Art der Verschlüsselung konfrontiert.

Konkrete Umsetzung

Den Schülern wird zunächst das Konzept der Vigenère-Verschlüsselung anhand eines Beispiels erläutert. Anschließend verfasst jeder Schüler eine kurze Botschaft und verschlüsselt sie nach dem gelernten Schema. Mithilfe des verwendeten Codeworts knackt nun der Banknachbar die Chiffrierung.

Methode der Verschlüsselung

Die Vigenère-Verschlüsselung basiert auf der (von der Caesar-Chiffre bekannten) Verschiebung des Alphabets. Dazu wird wieder im ersten Schritt das Alphabet notiert. Wieder wird der Klartext grün geschrieben.



Anschließend wird ein Codewort festgelegt (in unserem Beispiel das Wort „Natur“). Dessen Buchstaben bilden den jeweiligen Anfangsbuchstaben der roten Alphabete. Diese werden so untereinander geschrieben, dass eine eindeutige Zuordnung eines grünen Buchstaben mit je einem Buchstaben aus jedem roten Alphabet möglich ist. Der zu verschlüsselnde Text wird nun durchnummeriert. Dabei wird die höchste Zahl (nach der wieder von vorne begonnen wird) durch die Anzahl der Buchstaben des Codeworts vorgegeben (hier zählen wir also bis fünf). Die Verschlüsselung funktioniert nun wie die Caesar-Chiffrierung, wobei die Zahl eines Buchstaben das zu verwendende Alphabet vorgibt. Die Vorgehensweise lässt sich anhand der obigen Grafik gut nachvollziehen.

Erweiterung

Der Schwierigkeitsgrad der Entschlüsselung lässt sich in einer weiteren Übung deutlich erhöhen. Dazu wird ein vollständig verschlüsselter Text ausgeteilt, welcher etwa ein DinA4-Blatt füllt. Das Codewort wird in diesem Fall nicht vorgegeben. Mithilfe eines Tricks lässt sich jedoch dessen Länge bestimmen. Dazu wird der Text nach sich wiederholenden Buchstabenkombinationen abgesucht und deren Abstand ausgezählt. Meist handelt es sich dabei in der deutschen Sprache um häufig vorkommende Worte wie „und“, „der“, „die“ oder „das“. Bildet man nun den kleinsten gemeinsamen Teiler aller dieser Abstände, so erhält man die Länge n des Codeworts, da nach jeweils n Buchstaben wieder das selbe Alphabet verwendet wird. Die Zahl n gibt also die Periodizität der Verschlüsselung vor.
Im nächsten Schritt werden die Buchstaben des Werkes von Eins bis n durchnummeriert. Nun können alle gleich nummerierten Buchstaben als eigenständiger Text behandelt werden, der sich mithilfe der Wahrscheinlichkeitsanalyse entschlüsseln lässt.

Hintergründe

Durch Komplexität gewonnene Sicherheit

Im Vergleich zu den zuvor kennengelernten Verschlüsselungen, zeichnet sich die Vigenère-Chiffrierung durch ihre wesentlich höhere Sicherheit aus. Durch die Verwendung mehrerer Alphabete werden gleiche Buchstaben im Ausgangstext durch unterschiedliche Buchstaben in der Verschlüsselung repräsentiert, wodurch eine einfache Wahrscheinlichkeitsanalyse nicht zum Ziel führt. Den Schülern wird hier bewusst, dass der zusätzlich betriebene Aufwand lohnenswert ist, da der Schutz gegenüber unbefugten Lesern erheblich steigt.
Der einfachste Weg die Sicherheit zu erhöhen, ist die Verwendung eines längeren Codewortes. Es wäre gar denkbar, ganze Buchpassagen zu gebrauchen.
Die Länge des zu entschlüsselnden Textes wirkt sich dagegen in die andere Richtung aus: Je länger der Text, desto wahrscheinlicher wird es, viele sich wiederholende Buchstabenkombinationen zu finden und dadurch die Länge des Codewortes zu erhalten.Ein Teil der Komplexität der Vigenère-Chiffrierung besteht darin, dass diese tatsächlich eine Zusammensetzung mehrerer Caesar-Verschlüsselungen darstellt. Genauso gut ließe sich auch der Freimaurercode verwenden. Die Schüler können diesen Gedanken fortführen und verschiedene Verschlüsselungsarten kombinieren, um so eigene, sichere Methoden zu entwickeln. Das Erkennen der Zusammensetzbarkeit stimuliert somit die Kreativität und führt bestenfalls zu einer Art Wettbewerb, in dem die Schüler sich gegenseitig zu übertrumpfen versuchen. Im Zuge dessen ist es vorstellbar, dass sich die Kinder zuhause freiwillig noch intensiver mit dem Inhalt der Unterrichtsstunde beschäftigen, beispielsweise bei der Recherche nach weiterführenden Verschlüsselungsmethoden.