RSA & Co. in der Schule

Moderne Kryptologie, alte Mathematik, raffinierte Protokolle

Teil 2: Von Cäsar über Vigenère zu Friedman

von Helmut Witten, Irmgard Letzner und Ralph-Hardo Schulz

Im ersten Teil war von monoalphabetischen Chiffrierungen die Rede und davon, wie die Chiffrate bei hinreichender Länge des Textes mit Hilfe von Häufigkeitsanalysen zu entschlüsseln sind (vgl. LOG IN, 3/4'98, S. 57-65). Charakteristisch für diese Form der Verschlüsselung ist die eineindeutige Zuordnung von Zeichen des Klartextalphabets zu Zeichen des Geheimtextalphabets. Es ist ein naheliegender Gedanke, die Häufigkeitsmerkmale zu verschleiern, indem man im Klartext häufiger auftretenden Buchstaben mehrere verschiedene Geheimzeichen zuordnet. Eine derartige Verschlüsselung nennt man *homophon*. Im Idealfall tritt dann im Geheimtext jedes Zeichen gleich häufig auf. Eine Entschlüsselung, wie sie z. B. von Legrand im „Goldkäfer" von Edgar Allan Poe vorgenommen wird, ist dann nicht mehr möglich (vgl. LOG IN 3/4'98, S. 59 f.). Durch die Untersuchung der Häufigkeit von Bigrammen und Trigrammen (Folgen von zwei bzw. drei Zeichen) kann aber auch diese Chiffre mit statistischen Methoden gebrochen werden (vgl. z. B. Beutelspacher, [3]1993, S. 35 ff.). Trotzdem benutzte General L. R. Groves, der organisatorische Leiter des Manhattan-Projekts zur Entwicklung der amerikanischen Atombombe, noch im zweiten Weltkrieg eine solche homophone Verschlüsselung zur Übermittlung wichtiger Informationen (Kippenhahn, 1997, S. 129).

Historisch bedeutsamer sind jedoch die *polyalphabetischen Chiffrierungen*, die wir in dieser Folge am Beispiel des Verfahrens von Vigenère darstellen werden. Außerdem wollen wir ausführlich auf die Kryptoanalyse dieses Systems eingehen, die mit den Namen Kasiski und Friedman verbunden ist.

Zum besseren Verständnis des Vigenère-Verfahrens müssen wir aber zunächst einen Schritt zurückgehen und über die wohl bekannteste monoalphabetische Verschlüsselungsmethode sprechen, die auf den Imperator Cäsar zurückgeht. Wenn wir in unserer Artikelserie immer wieder auf solche einfachen Chiffren zu sprechen kommen, hat dies auch den Grund, daß sie sich in besonderer Weise für die Behandlung im Unterricht eignen.

Von Cäsar zu Vigenère

Der römische Historiker Sueton berichtet von vertraulichen Briefen, die Cäsar an Cicero und andere Bekannte schrieb. Dabei ersetzte er A durch D, B durch E usw.; er erhielt das Geheimtextalphabet (GTA) durch Verschiebung des normalen Alphabets (Klartextalphabet, KTA) um drei Stellen. Der Empfänger mußte dementsprechend in der umgekehrten Richtung schieben, um die Tabelle zur Entschlüsselung zu erhalten:

Verschlüsselung nach Cäsar

KTA:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GTA:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Diese Methode mag heute lächerlich einfach und unsicher erscheinen, wurde aber zur Freude der deutschen Kryptologen noch im ersten Weltkrieg von der russischen Armee verwendet (Bauer, 1995, S. 41). Vor 2000 Jahren aber waren statistische Methoden zur Untersuchung von Buchstabenhäufigkeiten noch völlig unbekannt. Das Verfahren erschien Cäsars Nachfolger Augustus sogar schon zu kompliziert, so daß er nach Suetons Bericht lediglich um einen Buchstaben verschob (vgl. Sgarro/Würmli, 1991, S. 9 ff.).

Verschlüsselung nach Augustus

KTA:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GTA:	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Das „Design" des Cäsar-Verfahrens ist auch heute noch lehrreich, denn es hat im Gegensatz zu Geheimschriften wie der vom Seeräuber Kidd (vgl. LOG IN 3/4'98, S. 59 f.) zwei entscheidende Vorteile:

▷ Das Geheimtextalphabet enthält keine Geheimzeichen, sondern nur die normalen Buchstaben. Ge-

heimzeichen bei einer monoalphabetischen Chiffrierung machen die Verschlüsselung komplizierter und das Chiffrat wirkt vielleicht für unbedarfte Betrachter geheimnisvoller, aber man erhält keinerlei echten Sicherheitsgewinn.

▷ Das Verfahren hat eine „eingebaute Variabilität" (Beutelspacher, 1997, S. 19); es definiert eine ganze *Klasse* von Verschlüsselungsverfahren, da man das A zu einem beliebigen anderen Buchstaben verschieben kann. So erhält man bei 26 Buchstaben 25 Verschlüsselungsarten (wenn man von der identischen Abbildung absieht).

Damit kann man schon bei diesen einfachen *Verschiebechiffren* zwischen dem *Algorithmus* (das Geheimtextalphabet entsteht durch Verschiebung des Klartextalphabets) und dem *Schlüssel* unterscheiden (bei Cäsar D, bei Augustus B etc.).

Ein offensichtlicher Nachteil der Verschiebe-Chiffren soll nicht verschwiegen werden: Wegen der geringen Zahl von Schlüsseln kann man den Geheimtext auch ohne statistische Analyse durch bloßes Probieren dechiffrieren. Abhilfe versprechen hier die sog. *Tauschchiffren*, die man z. B. durch ein *Schlüsselwort* erhält (s. u.). Dabei wird das Schlüsselwort unter einen bestimmten Buchstaben des Klartextalphabets geschrieben (in unserem Beispiel unter das D), doppelt vorkommende Zeichen werden beim zweiten Auftreten gestrichen (in unserem Beispiel das zweite I von **IN**FORMATIK) und der Rest des Geheimtextalphabets mit den verbleibenden Buchstaben aufgefüllt:

Verschlüsselung mit dem Schlüsselwort INFORMATIK und dem Startbuchstaben D

```
KTA: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
GTA: X Y Z I N F O R M A T K B C D E G H J L P Q S U V W
```

Durch diese einfache Modifikation des Cäsar-Verfahrens erhält man eine gewaltige Vergrößerung des Schlüsselraumes: Statt 26 hat man damit die nahezu unvorstellbare Zahl von

26! = 403 291 461 126 605 635 584 000 000

möglichen Verschlüsselungen (einschließlich der Identität), wobei allerdings die meisten der „Schlüsselwörter" irgendwelche beliebigen Vertauschungen *(Permutationen)* der 26 Buchstaben des Klartextalphabets sind. Rechnet man diese riesige Zahl auf die Weltbevölkerung von z. Z. knapp 6 Milliarden um, bleiben noch für jeden Erdbewohner über 67 Billarden mögliche Schlüsselwörter.

Die riesige Zahl möglicher Schlüssel sollte aber nicht über die Schwäche aller monoalphabetischen Chiffrierungen von Texten einer natürlichen Sprache hinwegtäuschen: Durch die in der ersten Folge unserer Artikelserie vorgestellte statistische Analyse sind sie relativ einfach zu „knacken".

Mehr Sicherheit bieten die *polyalphabetischen* Chiffrierungen, die zur Zeit der Renaissance von dem Mönch Johannes Trithemius (1462-1516), dem Diplomaten Blaise de Vigenère (1523-1596) und anderen erfunden und die z. T. bis ins 20. Jahrhundert professionell genutzt wurden. Ausgangspunkt der beiden Verschlüsselungsverfahren von Trithemius und Vigenère ist eine quadratische Tafel mit den 26 Verschiebechiffren (einschließlich der identischen) nach Cäsar (s. Bild 1). Diese Tafel wurde zuerst in einem posthum veröffentlichten Buch von Trithemius abgedruckt.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Bild 1: Die Trithemius- oder Vigenère-Tafel.

Trithemius schlug vor, den ersten Buchstaben des Klartextes nach der ersten Zeile, den zweiten nach der zweiten Zeile usw. zu verschlüsseln. Nach 26 Buchstaben sollte man wieder von vorne beginnen. Von diesem Verfahren ist es nur noch ein kleiner Schritt zur Vigenère-Chiffre.

Die Vigenère-Verschlüsselung

Blaise de Vigenère (Bild 2, nächste Seite) war fast sein ganzes Leben lang Diplomat in den Diensten des Herzogs von Nevers. Er studierte die Werke von Trithemius und anderen über Geheimschriften; in Rom traf er mit den in ihrer Disziplin führenden Kryptologen des Papstes zusammen und entwickelte verschiedene eigene Chiffriersysteme. In seinem berühmten Buch „Traité des chiffres" (1586) faßte er die kryptographischen Erkenntnisse seiner Zeit zusammen. Dieses Buch geriet nach seinem Tod in Vergessenheit, und erst im 19. Jahrhundert wurde man wieder auf die Schriften Vigenères aufmerksam (Kippenhahn, 1997, S. 142).

Wie erfolgt nun die Verschlüsselung nach Vigenère? Im Gegensatz zu Trithemius benutzte Vigenère zusätzlich zu der quadratischen Tafel ein Schlüsselwort, so daß man wie bei Cäsar klar zwischen Algorithmus und

Quelle: Sgarro/Würmli, 1991, S. 47

Bild 2: Blaise de Vigenère (1523–1596), französischer Diplomat und bedeutender Kryptologe.

Schlüssel trennen kann. Gleichzeitig wird durch diese Modifikation die Entzifferung erschwert – aber nicht unmöglich (s. u.)!

Die Methode soll anhand des Schlüsselwortes KRYPT und dem zu verschlüsselnden Text LOGIN erläutert werden. Man sucht den ersten Buchstaben des Klartextes in der ersten Zeile der Vigenère-Tafel (im Beispiel: L) und den ersten Buchstaben des Schlüsselwortes in der ersten Spalte der Vigenère-Tafel (im Beispiel: K) und ersetzt den Buchstaben des Klartextes durch den Buchstaben, den man an der Kreuzung der gefundenen Zeile und Spalte findet (im Beispiel: L wird durch V ersetzt). Die Vigenère-Tafel wird also wie eine Verknüpfungstafel benutzt. Analog verfährt man mit den übrigen Buchstaben des Klartextes. Hat das Schlüsselwort weniger Zeichen als der Klartext, so benutzt man dasselbe Schlüsselwort wiederholt. (Aus Symmetriegründen kann die Rolle von Zeilen und Spalten vertauscht werden.)

In der Vigenère-Tafel ergibt sich für die ersten drei Buchstaben unseres Beispiels das Bild 3.

Unser Beispiel ergibt nach diesem Schema:

Schlüsselwort:	K R Y P T
Klartext:	L O G I N
Verschlüsselter Text:	V F E X G

Ein anderes Beispiel macht den Unterschied zu monoalphabetischen Verschlüsselungen deutlich:

Schlüsselwort:	O T T O O T T O
Klartext:	M I N I M I D I
Verschlüsselter Text:	A B G W A B W W

Derselbe Buchstabe im Klartext kann unterschiedlich verschlüsselt werden je nach der Stelle, an der er unter dem Schlüsselwort steht (im Beispiel: Aus I wird B und W). Andererseits können verschiedene Buchstaben, wenn sie an unterschiedlichen Stellen unter dem Schlüsselwort stehen, durch dasselbe Zeichen ersetzt werden (im Beispiel: Aus I und D des Klartextes wird hier W im Geheimtext – vgl. Bild 4, nächste Seite).

Beide Eigenschaften erschweren die Entschlüsselung erheblich. Das Verfahren ist um so sicherer, desto länger das Schlüsselwort ist. Im Idealfall wählt man das Schlüsselwort so lang wie den Klartext. Perfekte Sicherheit erhält man, wenn das Schlüsselwort eine Zufallsfolge von der Länge des Klartextes ist. Das so gewonnene hohe Maß an Sicherheit hat seinen Preis: Die Übermittlung des Schlüssels wird sehr aufwendig. Wir werden dieses System von VERNAM, das auch „one-time-pad"-Verfahren genannt wird, in der nächsten Folge unserer Artikelserie besprechen.

Bild 3: Verschlüsselung mit der Vigenère-Tafel.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	M	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Der Kasiski-Test – Kryptoanalyse zum ersten

Es hat fast 300 Jahre gedauert, bis ein Verfahren zur Entschlüsselung von nach Vigenère codierten Texten entwickelt wurde. 1863 veröffentlichte Friedrich W. Kasiski (1805-1881), ein ostpreußischer Offizier, im Büchlein „Die Geheimschriften und die Dechiffrierkunst" seine Idee und Anleitung. Kasiski betätigte sich nur kurz als Kryptologe, da sein Buch kaum Beachtung fand. Später beschäftigte er sich mit dem Ausgraben vorgeschichtlicher Gräber und veröffentlichte darüber in Fachzeitschriften. Vermutlich hat er nie erfahren, daß er die Kryptologie revolutioniert hat (Kippenhahn, 1997, S. 151).

Wenn das Schlüsselwort bekannt ist, stellt die Decodierung eines nach Vigenère verschlüsselten Geheimtextes kein Problem dar. Die bahnbrechende Idee von Kasiski war, daß bereits die Kenntnis der Schlüsselwort*länge* ausreicht, um einen hinreichend langen Text zu entziffern. Verfolgen wir zunächst diesen Gedanken, ehe wir uns dazu äußern, wie man die Schlüsselwortlänge ermittelt.

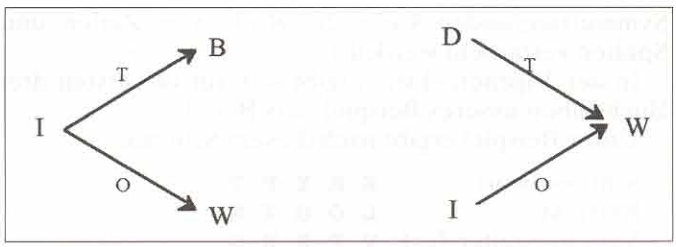


Bild 4: Polyalphabetische Verschlüsselung – gleiche Buchstaben des Klartextes können auf unterschiedliche Buchstaben des Geheimtextes führen, unterschiedliche Buchstaben des Klartextes können auf gleiche Buchstaben des Geheimtextes führen.

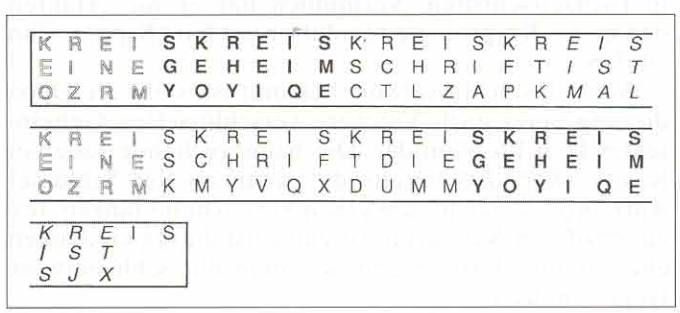
Alle Zeichen, die unter demselben Buchstaben des Schlüsselworts stehen, werden durch dieselbe Zeile in der Vigenère-Tafel codiert. Alle Zeichen, die unter dem ersten Buchstaben des Schlüsselwortes stehen, werden also monoalphabetisch verschlüsselt, ebenso alle Zeichen, die unter dem zweiten Buchstaben des Schlüsselwortes stehen, usw. Sucht man unter den gleichartig verschlüsselten Zeichen das am häufigsten auftretende heraus, so weiß man, daß dieser Buchstabe mit großer Wahrscheinlichkeit aus dem E des Klartextes entstanden ist. Mit dem E des Klartextes und dem zugehörigen Buchstaben des codierten Textes läßt sich das Zeichen des Schlüsselwortes rekonstruieren. Ebenso verfährt man mit den zweiten, den dritten, ... Buchstaben des Schlüsselwortes.

Die Bestimmung des Schlüsselwortes ist allerdings der zweite Schritt vor dem ersten. Zunächst benötigt man die Schlüsselwort*länge*. Folgender Gedanke liegt der Ermittlung der Schlüsselwortlänge zugrunde: Aus gleichen Zeichenfolgen im Klartext an derselben Stelle des Schlüsselwortes werden gleiche Zeichenfolgen im Geheimtext. Entstehen umgekehrt im verschlüsselten Text gleiche Buchstabenfolgen, so steht der zugehörige Klartext wahrscheinlich unter denselben Zeichen des Schlüsselwortes (im Beispiel aus Bild 5: Die Zeichenfolge OZRM tritt zweimal auf. Sie entsteht beide Male durch KREI aus EINE.). Das geschieht aber genau dann, wenn „zwischen" den Wiederholungen im verschlüsselten Text (bzw. im Klartext) das Schlüsselwort mehrfach auftritt, wobei vom ersten Zeichen der doppelt auftretenden Folgen bis vor den ersten Buchstaben der Wiederholung gezählt wird. In diesem Fall ist die Anzahl der Zeichen „zwischen" den Wiederholungen, die man auch *Kasiski-Abstand* nennt, ein Vielfaches der Schlüsselwortlänge. (Im Beispiel: Der Kasiski-Abstand von OZRM beträgt 20, dies ist ein Vielfaches der Schlüsselwortlänge 5.)

Treten mehrere Wiederholungen auf, so bestimmt man jedesmal den Kasiski-Abstand. Die Länge des Schlüsselwortes ist dann um so wahrscheinlicher ein gemeinsamer Teiler der Abstände, desto mehr solcher Wiederholungen gefunden werden und desto länger sie sind. (Im Beispiel: Der Kasiski-Abstand von YOYIQE beträgt 30. Die Zahl 30 ist ebenfalls ein Vielfaches der Schlüsselwortlänge 5.) Einen längeren Geheimtext zur Dechiffrierung nach Kasiski finden Sie weiter unten (S. 38 – Bild 10).

Leider treten beim Kasiski-Test auch „unechte" Parallelstellen auf, die man von vornherein nicht als solche erkennen kann. Eine sensiblere Methode, die Periodenlänge bei einem periodisch polyalphabetisch chiffrierten Text zu bestimmen, stammt von dem amerikanischen Kryptologen William F. Friedman (1891-1969).

Bild 5: Parallelstellen in einem nach Vigenère verschlüsselten Text ermöglichen die Ermittlung der Schlüsselwortlänge.



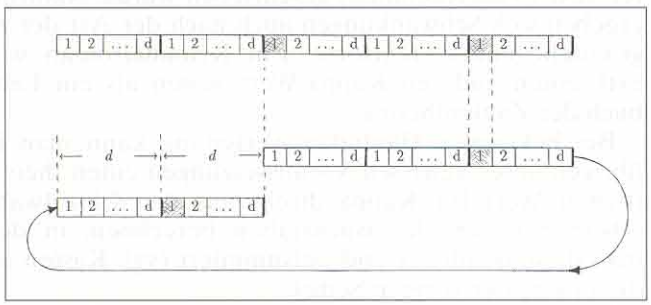
Der Friedman-Test – Kryptoanalyse zum zweiten

Friedman ist einer der berühmtesten Kryptologen aller Zeiten. Als Kind russischer Immigranten mußte er sein Studium der Genetik an der Cornell-Universität (New York) als Kellner selbst finanzieren. Seine erste Anstellung erhielt er 1915 bei dem wohlhabenden Textilkaufmann und Mäzen George Fabyan, der den jungen Wissenschaftler engagierte, um mit seiner Hilfe die Ernteerträge seiner Pflanzungen zu verbessern. Außerdem war Fabyan von der Idee besessen, an Shakespeares Werken nachzuweisen, daß diese in Wirklichkeit von Sir Francis Bacon geschrieben worden seien. Zu diesem Zweck beschäftigte er auch einige Kryptologen. „Friedman fand dort Interesse an Elizabeth Smith, einer jungen Kryptologin, und an der Kryptologie. Er verheiratete sich mit beiden und wurde der erfolgreichste amerikanische Kryptologe" (Bauer, 1995, S. 26; Kippenhahn, 1997, S. 43 ff.). Den Nachweis, daß Shakespeare und Bacon identisch sind, konnte Friedman allerdings nicht erbringen. (Er war wie seine Frau zu der Überzeugung gelangt, daß diese These nicht stimmen kann; das Ehepaar Friedman hat später ein Buch darüber geschrieben.)

Bald war er als Experte so bekannt geworden, daß die Marine ihn 1924 bat, den Code der Marsbewohner zu brechen – man hielt etwas für Signale der „grünen Männchen", das sich später als Funkstörung erwies. 1929 wurde Friedman zum Leiter der neugegründeten Chiffrierabteilung der amerikanischen Armee berufen, die zu Beginn des kalten Krieges in die berühmte NSA

Der Friedman-Test (Teil I): Mathematische Grundlagen

Der Friedman-Test nutzt aus, daß Parallelstellen in einem chiffrierten Text bei entsprechender *zyklischer Verschiebung* zu Übereinstimmungen führen (s. nachfolgendes Bild), die sich zahlenmäßig erfassen lassen.



Chiffrat der Schlüsselwort-Länge d vor und nach der zyklischen Verschiebung um 2-fache Periodenlänge (mit Markierung der Position i der Buchstaben des Schlüsselwortes, i = 1, ..., d, und schraffierten Parallelstellen bei i = 1).

Um generell die Übereinstimmungen zwischen zwei Texten messen zu können, ist es nützlich, eine Größe, die sogenannte *Zeichenkoinzidenz-Häufigkeit „Kappa"*, zu definieren, zunächst für zwei beliebige Texte (gleicher Länge).

Definition: Seien $T = t_1 \ldots t_M$ und $T' = t'_1 \ldots t'_M$ zwei Texte gleicher Länge M über demselben Alphabet. Dann beschreibt

$$\text{Kappa}(T,T') := \frac{1}{M} \sum_{i=1}^{M} \delta(t_i, t'_i)$$

(mit Indikatorfunktion δ : $\delta(x,y) = 1$ für $x = y$ und $\delta(x,y) = 0$ für $x \neq y$) die relative Häufigkeit der Übereinstimmung in den „übereinandergelegten" Texten.

Beispiel: Kappa (OTTO, TOTO) $= \frac{1}{4}(0+0+1+1) = \frac{1}{2}$.

Wir untersuchen den *Erwartungswert für das Kappa* zweier Texte der Länge M von stochastischen Quellen Q und Q′ mit gleichem Alphabet, aber evtl. verschiedener Zeichenwahrscheinlichkeit $p(x_j) = p_j$ in Q und $p(x_j) = p'_j$ in Q′ (für j = 1, ..., N). Es gilt für (zunächst als voneinander unabhängig angenommene) Texte $T = t_1, t_2, \ldots, t_M$ und $T' = t'_1, t'_2, \ldots, t'_M$:

$$E(\text{Kappa}(T,T') \mid T \text{ aus Quelle Q und } T' \text{ aus Quelle Q}')$$

$$= E\left(\frac{1}{M}\sum_{i=1}^{M} \delta(t_i, t'_i)\right) \underset{\text{E linear}}{=} \frac{1}{M}\sum_{i=1}^{M} E(\delta(t_i, t'_i))$$

$$= \frac{1}{M}\sum_{i=1}^{M}\left(\sum_{j=1}^{N} p(t_i = x_j \text{ und } t'_i = x_j)\right)$$

$$= \frac{1}{M} \cdot M \cdot \sum_{j=1}^{N} p_j p'_j = \sum_{j=1}^{N} p_j p'_j .$$

Sind die beiden Quellen gleich, Q = Q′, und die Texte T und T′ voneinander unabhängig, so ergibt sich speziell

$$\kappa_Q := E(\text{Kappa}(T,T'))_Q = \sum_{j=1}^{N} p_j^2 .$$

Aus den relativen Buchstabenhäufigkeiten der englischen bzw. deutschen Sprache läßt sich der Erwartungswert für das Kappa zweier Texte mittels

$$\kappa_Q := E(\text{Kappa}(T,T'))_Q = \sum_{j=1}^{N} p_j^2 \quad \text{(s. oben) berechnen;}$$

man erhält $\kappa_{\text{Deutsch}} = 0{,}07619$ und $\kappa_{\text{Englisch}} = 0{,}06577$.

Dies sind die theoretischen Werte für die empirisch aus langen Texten gewonnenen Werte κ_{Deutsch} bzw. κ_{Englisch}. Bei einer Quelle, die die 26 Buchstaben des Alphabets mit Gleichverteilung sendet ($p_j = \frac{1}{26} = \frac{1}{N}$ für alle j), ist hingegen $\kappa_{\text{Gleichverteilung}} = 26 \cdot (\frac{1}{26})^2 = \frac{1}{26} \approx 0{,}03846$.

Man stellt also einen deutlichen Unterschied zu den Werten κ_{Deutsch} und κ_{Englisch} fest.

Für identische Quellen Q = Q′ mit Alphabet A und |A| = N gilt, wie man zeigen kann, $\frac{1}{N} \leq \kappa_Q \leq 1$.

Die linke Grenze wird bei der Gleichverteilung angenommen, die rechte Grenze bei deterministischer Verteilung (d. h. $p_j = 1$ für ein j und $p_i = 0$ sonst, also bei einer Quelle, die stets das Zeichen x_j liefert).

Teil II nächste Seite

(*N*ational *S*ecurity *A*gency) umgewandelt wurde. Im zweiten Weltkrieg gelang unter seiner Leitung die Kryptoanalyse des Codes der „Purple" (dem japanischen Gegenstück zur deutschen Enigma).

Bereits zu Beginn der zwanziger Jahre hatte Friedman Methoden der modernen Statistik in die Kryptologie eingeführt. Am bekanntesten wurde der von ihm entwickelte Kappa-Test zur Bestimmung der Schlüsselwortlänge bei der Vigenère-Chiffrierung. Ihm zu Ehren erhielt dieses Verfahren den Namen Friedman-Test (vgl. den Kasten auf dieser und der nächsten Seite mit einer mathematisch exakten Beschreibung).

Der von Friedman eingeführte Koinzidenzindex κ (ein kleines griechisches Kappa) ist leicht zu verstehen: Man legt zwei Texte gleicher Länge übereinander und zählt die Stellen, an denen Buchstaben übereinstimmen, anschließend teilt man diese Anzahl durch die Gesamtzahl der vorkommenden Buchstaben.

Damit kann man sofort eine obere Schranke angeben: Kappa kann höchstens eins werden (wenn die Texte identisch sind). Hat man dagegen willkürlich zusammengewürfelte Buchstabensalate, wird sich im Durchschnitt nur bei jedem 26. Buchstaben eine Übereinstimmung ergeben, Kappa ist hier also ungefähr 1/26 ≈ 3,85 %.

Texte natürlicher Sprachen sind alles andere als gleichverteilt (vgl. z. B. LOG IN, 3/4'98, S. 61 f.); für diese ist Kappa etwa doppelt so groß wie bei einem Zu-

Der Friedman-Test (Teil II): Anwendung von Kappa

Betrachtet wird ein nach Vigenère verschlüsselter Text T und dessen zyklische Verschiebungen T^u für u = 1,2,3, ... Ist u = kd ein Vielfaches der Periodenlänge d, so kann man davon ausgehen, daß T und T^u komponentenweise aus derselben Quelle stammen, da die zugehörigen Klartexte P und P^{kd} an jeder Stelle i derselben monoalphabetischen Substitution c_i unterworfen wurden und

$$\sum_{j=1}^{N} p_j^2$$

nicht von der Reihenfolge der p_j abhängig ist. Setzen wir vereinfachend voraus, daß bei T die einzelnen Stellen im wesentlichen unabhängig voneinander sind, so ergibt sich (vgl. auch den Kasten auf der vorigen Seite über den Erwartungswert von Kappa):

$$E\,(\text{Kappa}\,(T, T^{kd})) = \frac{1}{M}\sum_{i=1}^{M}\sum_{j=1}^{N} p\,(t_i = x_j)^2$$

$$= \frac{1}{M}\sum_{i=1}^{M}\sum_{j=1}^{N} p_j^2 = \sum_{j=1}^{N} p_j^2 \doteq \kappa_Q$$

(mit den Wahrscheinlichkeiten p_j der Zeichen der chiffrierten Quelle Q).

Ist hingegen u kein Vielfaches der Periode d, so lassen sich unter gewissen Voraussetzungen (z. B. genügend gründlicher Durchmischung der Zeichenhäufigkeit) die Texte T und T^u als aus stochastisch unabhängigen Quellen entstanden annehmen und Kappa in der Nähe von $\kappa_{\text{Gleichverteilung}}$ erwarten.

Wir wollen also die folgende Aussage begründen:

Ist die Schlüsselwortlänge kein Teiler von u, so gilt annähernd $E\,(\text{Kappa}\,(T,T^u)) = \kappa_{\text{Gleichverteilung}}$.

Wie oben gesehen, gilt für einen Text der Länge M:

$$E = E\,(\text{Kappa}\,(T, T^u)) = \frac{1}{M}\sum_{i=1}^{M}\sum_{j=1}^{N} p\,(t_i = x_j \text{ und } t_i' = x_j);$$

eine Umbenennung des Alphabets an der i-ten Stelle ändert nichts, da über alle x_j für j = 1, ..., N summiert wird; wir ändern die Bezeichnung so, daß $p(t_i = x_j) = p_j$ gilt, und erhalten

$$E = \frac{1}{M}\sum_{j=1}^{N}\sum_{i=1}^{M} p_j \cdot p\,(t_i' = x_j) = \frac{1}{M}\sum_{j=1}^{N} p_j \sum_{i=1}^{M} p\,(t_i' = x_j).$$

Ist die Chiffrierung so gut durchmischt, daß $\{p(t_1' = x_j), \ldots, p(t_M' = x_j)\} \doteq \{p_1, \ldots, p_N\}$ für jeweils einen Text der Länge M = N gilt, (d. h., daß durch die Chiffrierung jedes Zeichen des Alphabets mit der Wahrscheinlichkeit jedes anderen Zeichens der Quelle an einer Stelle des Textes T′ auftritt), so folgt

$$E\,(\text{Kappa}\,(T, T')) = \frac{1}{N}\sum_{j=1}^{N} p_j \cdot 1 = \frac{1}{N} = \kappa_{\text{Gleichverteilung}}.$$

fallstext. Umfangreiche statistische Untersuchungen ergeben für deutschsprachige Texte einen Wert von 7,62 %, im Englischen erhält man 6,58 % während für russische Texte (bei 32 Buchstaben des kyrillischen Alphabets) ein Wert von 5,29 % charakteristisch ist (Bauer, 1995, S. 249). Da man Kappa sehr leicht berechnen kann, wird dieser Index auch dafür genutzt, mit Computern die Sprache zu ermitteln, in der ein unbekannter Text (wahrscheinlich) geschrieben wurde. Natürlich ergeben sich Schwankungen auch nach der Art der zugrundeliegenden Textsorte: Ein Kriminalroman wird evtl. einen anderen Kappa-Wert haben als ein Lehrbuch der Zahlentheorie.

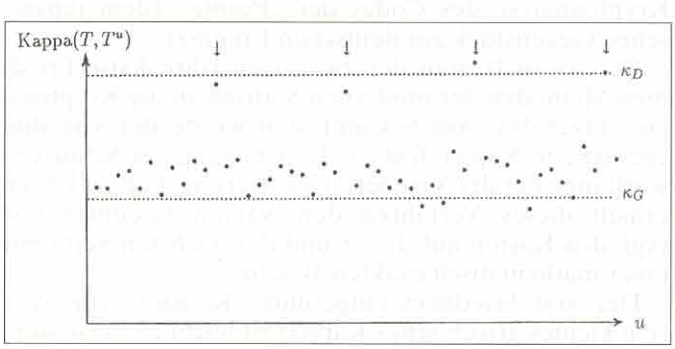
Bei bekannter Häufigkeitsverteilung kann man im übrigen unter gewissen Voraussetzungen einen theoretischen Wert für Kappa direkt aus den Einzelwahrscheinlichkeiten der Buchstaben berechnen, in dem man diese quadriert und aufsummiert (vgl. Kasten auf dieser und der vorigen Seite).

Eine erste kryptologische Anwendung von Kappa ergibt sich aus der Tatsache, daß sich die Häufigkeitsverteilung bei monoalphabetischer Chiffrierung nicht verändert, während bei der polyalphabetischen Chiffrierung die Häufigkeiten der einzelnen Buchstaben angenähert werden. Im ersten Fall wird Kappa also den Werten für die zugrundeliegenden natürlichen Sprachen entsprechen, im zweiten wird Kappa dagegen näher bei dem Wert für die Gleichverteilung liegen.

Der geniale Gedanke von Friedman war nun, den chiffrierten Text T buchstabenweise gegen sich selbst zu verschieben und für jede mögliche Verschiebung u den Wert von Kappa(T,T^u) auszurechnen (dabei bezeichnet T^u den um u zyklisch verschobenen Text T – s. Bild im Kasten auf der vorigen Seite). Wenn der Versatz u der beiden Texte ein Vielfaches der Schlüssellänge ist, stehen jeweils Buchstaben übereinander, die nach demselben Cäsar-Alphabet chiffriert wurden. In diesen Fällen wird Kappa den Werten für die natürliche Sprache entsprechen, sonst ist er deutlich niedriger (etwa in der Nähe des Wertes für die Gleichverteilung; vgl. Bild 6).

Als Beispiel betrachten wir den schon beim Kasiski-Test untersuchten Geheimtext:

Bild 6: Werte von Kappa(T,T^u) bei zyklischer Verschiebung eines periodisch polyalphabetisch chiffrierten Textes T der Länge M = 3000 um u Stellen mit κ_G = 0,03846 (Gleichverteilung), κ_D = 0,07619 (Deutsch).



Quelle: Bauer, 1995, S. 260

u	T^u	K
0	OZRMYOYIQE CTLZAPKMAL OZRMKMYVQX DUMMYOYIQE SJX	
1	XOZRMYOYIQ ECTLZAPKMA LOZRMKMYVQ XDUMMYOYIQ ESJ	1
2	JXOZRMYOYI QECTLZAPKM ALOZRMKMYV QXDUMMYOYI QES	3
3	SJXOZRMYOY IQECTLZAPK MALOZRMKMY VQXDUMMYOY IQE	0
4	ESJXOZRMYO YIQECTLZAP KMALOZRMKM YVQXDUMMYO YIQ	1
5	QESJXOZRMY OYIQECTLZA PKMALOZRMK MYVQXDUMMY OYI	1
6	IQESJXOZRM YOYIQECTLZ APKMALOZRM KMYVQXDUMM YOY	1
7	YIQESJXOZR MYOYIQECTL ZAPKMALOZR MKMYVQXDUM MYO	2
8	OYIQESJXOZ RMYOYIQECT LZAPKMALOZ RMKMYVQXDU MMY	6
9	YOYIQESJXO ZRMYOYIQEC TLZAPKMALO ZRMKMYVQXD UMM	1
10	MYOYIQESJX OZRMYOYIQE CTLZAPKMAL OZRMKMYVQX DUM	1
11	MMYOYIQESJ XOZRMYOYIQ ECTLZAPKMA LOZRMKMYVQ XDU	1
12	UMMYOYIQES JXOZRMYOYI QECTLZAPKM ALOZRMKMYV QXD	1
13	DUMMYOYIQE SJXOZRMYOY IQECTLZAPK MALOZRMKMY VQX	8
14	XDUMMYOYIQ ESJXOZRMYO YIQECTLZAP KMALOZRMKM YVQ	2
15	QXDUMMYOYI QESJXOZRMY OYIQECTLZA PKMALOZRMK MYV	4
16	VQXDUMMYOY IQESJXOZRM YOYIQECTLZ APKMALOZRM KMY	1
17	YVQXDUMMYO YIQESJXOZR MYOYIQECTL ZAPKMALOZR MKM	0
18	MYVQXDUMMY OYIQESJXOZ RMYOYIQECT LZAPKMALOZ RMK	0
19	KMYVQXDUMM YOYIQESJXO ZRMYOYIQEC TLZAPKMALO ZRM	0
20	MKMYVQXDUM MYOYIQESJX OZRMYOYIQE CTLZAPKMAL OZR	6
21	RMKMYVQXDU MMYOYIQESJ XOZRMYOYIQ ECTLZAPKMA LOZ	2
22	ZRMKMYVQXD UMMYOYIQES JXOZRMYOYI QECTLZAPKM ALO	2
23	OZRMKMYVQX DUMMYOYIQE SJXOZRMYOY IQECTLZAPK MAL	7
24	LOZRMKMYVQ XDUMMYOYIQ ESJXOZRMYO YIQECTLZAP KMA	0
25	ALOZRMKMYV QXDUMMYOYI QESJXOZRMY OYIQECTLZA PKM	0
26	MALOZRMKMY VQXDUMMYOY IQESJXOZRM YOYIQECTLZ APK	0
27	KMALOZRMKM YVQXDUMMYO YIQESJXOZR MYOYIQECTL ZAP	1
28	PKMALOZRMK MYVQXDUMMY OYIQESJXOZ RMYOYIQECT LZA	4
29	APKMALOZRM KMYVQXDUMM YOYIQESJXO ZRMYOYIQEC TLZ	2
30	ZAPKMALOZR MKMYVQXDUM MYOYIQESJX OZRMYOYIQE CTL	8
	usw.	
42	ZRMYOYIQEC TLZAPKMALO ZRMKMYVQXD UMMYOYIQES JXO	1

Bild 7: Beispiele von Kappa-Werten κ = K/43 bei zyklischer Verschiebung um u.

OZRMYOYIQECTLZAPKMALOZRMKMYVQXDUMMYOYIQESJX

Wir verschieben nun um 1, 2, 3, ... Positionen und kontrollieren die Anzahl der Übereinstimmungen. Auffällig sind z. B. die Werte u = 8, 13, 15, 20, 23, 28, 30; Unter diesen Werten und den Abständen zwischen ihnen kommen Vielfache der Schlüsselwortlänge 5 vor, aber auch andere Zahlen (Bild 7).

Diese erhaltenen Kappa-Werte entsprechen nicht ganz unseren Erwartungen. Dazu muß man aber bedenken, daß der Text nur die Länge 43 hat, so daß durch jeden Buchstaben des Schlüsselwortes höchstens 9 Buchstaben des Klartextes verschlüsselt werden. Dies ist für eine statistische Analyse keine sichere Grundlage. Hinzu kommt, daß bei der letzten Verwendung des Schlüsselwortes zum Chiffrieren zwei Buchstaben nicht benötigt werden. Damit gibt es auch einen Block der Länge 3 zusätzlich zu 8 Blöcken der Länge 5. In Bild 8 wird an einem kürzeren Beispiel (mit der Kryptogrammlänge M = 13) gezeigt, daß bei der Schlüsselwortlänge 5 auch Verschiebungen um 3 = M – 10 und 8 = M – 5 Schritte zu Übereinstimmungen führen. Dieses Phänomen macht sich erst dann nicht mehr störend bemerkbar, wenn das Kryptogramm wesentlich länger ist als das Schlüsselwort.

Um längere Texte zu untersuchen, bietet sich die Verwendung eines Programms an. Im LOG IN-Service können Sie ein Turbo-PASCAL-Programm erhalten, bei dem der Kappa-Verlauf automatisch ermittelt wird. Bei dem Beispiel aus dem Arbeitsbogen (s. S. 38) werden als Verschiebungen mit einem Koinzidenzindex größer oder gleich 8 % für u die Werte 14, 21, 28, 49 und 77 ausgegeben, so daß in diesem Fall die Schlüsselwortlänge 7 als größter gemeinsamer Teiler (ggT) dieser Zahlen eindeutig bestimmt werden kann. Da dieses Chiffrat M = 746 Buchstaben umfaßt, macht sich der störende Effekt aus dem ersten Beispiel nicht mehr bemerkbar, obwohl auch bei diesem Text M kein Vielfaches der Schlüsselwortlänge ist.

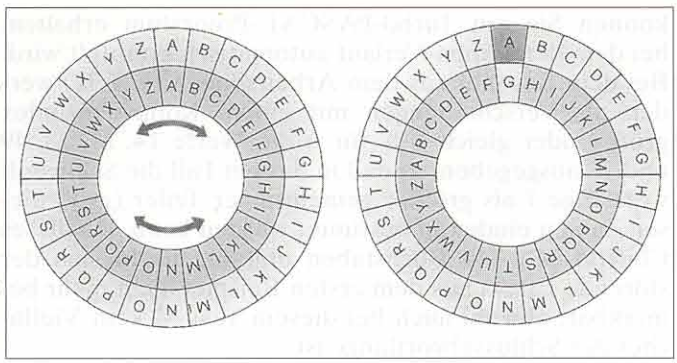
Hinweise für den Mathematikunterricht

Es ist sicherlich kein Zufall, daß fast alle Kryptologie-Bücher mit der Cäsar-Chiffrierung anfangen – auch im Unterricht ist dies ein guter Einstieg. Besonders leicht wird das Ver- und Entschlüsseln nach einer Verschiebechiffre, wenn man dafür eine Scheibe benutzt. Cäsar kannte eine solche Scheibe (wahrscheinlich) noch nicht, sie wurde zuerst von Leon Battista Alberti (1404-1472) in seinem Buch „Modus scribendi in ziferas" beschrieben (Bild 9, nächste Seite).

Eine Alberti-Scheibe kann auch für die Vigenère-Ver- oder Entschlüsselung genutzt werden, indem man bei jedem Buchstaben des Schlüsselwortes die Scheibe entsprechend verdreht. Umgekehrt kann man die Caesar-Verschlüsselung mit Hilfe der Vigenère-Tafel realisieren: Man sucht in der ersten Zeile den Klartext und in der vierten Zeile den Geheimtext. Die Lernenden üben den Umgang mit dieser Tafel, indem sie z. B.

Bild 8: Zyklische Verschiebung eines Textes der Länge M = 13 um u mit der Schlüsselwortlänge 5. Die Zahlen geben die Positionen der Schlüsselwort-Buchstaben an.

u = 0	1	2	3	4	5	1	2	3	4	5	1	2	3
u = 1	3	1	2	3	4	5	1	2	3	4	5	1	2
u = 2	2	3	1	2	3	4	5	1	2	3	4	5	1
u = M-10	1	2	3	1	2	3	4	5	1	2	3	4	5
u = 4	5	1	2	3	1	2	3	4	5	1	2	3	4
u = 5	4	5	1	2	3	1	2	3	4	5	1	2	3
u = 6	3	4	5	1	2	3	1	2	3	4	5	1	2
u = 7	2	3	4	5	1	2	3	1	2	3	4	5	1
u = M-5	1	2	3	4	5	1	2	3	1	2	3	4	5
u = 9	5	1	2	3	4	5	1	2	3	1	2	3	4
u = 10	4	5	1	2	3	4	5	1	2	3	1	2	3
u = M-2	3	4	5	1	2	3	4	5	1	2	3	1	2
u = M-1	2	3	4	5	1	2	3	4	5	1	2	3	1



Quelle: Sgarro/Würmli, 1991, S. 19

Bild 9: Chiffrierscheiben nach Alberti: Auf der Scheibe rechts wird der Buchstabe A des Klartextes durch den Buchstaben G verschlüsselt, das B durch das H usw.

Aufgaben zu unterschiedlichen Verschiebe-Chiffren lösen.

Die Verschiebechiffren machen – wie bereits erwähnt – einem potentiellen Lauscher natürlich nur äußerst geringfügige Probleme, da es (einschließlich der identischen) nur 26 Verschiebungen gibt. Außerdem hat man mit einem Buchstaben auch alle anderen entziffert.

Das Verschlüsseln eines Textes nach Vigenère sowie die Entschlüsselung kann bei Kenntnis des Schlüsselwortes von den Schülern mit Hilfe der quadratischen Tafel leicht bewältigt werden. Als Übung gut geeignet ist hier Partnerarbeit: Jeder Schüler verschlüsselt einen (kurzen) eigenen Text und übermittelt ihn zusammen mit dem Codewort seinem Partner zum Entschlüsseln.

Mühsamer, aber auch reizvoller, ist die Entschlüsselung, wenn das Schlüsselwort nicht bekannt ist. Bei dem Kasiski-Verfahren gilt es zunächst, gleichartige Buchstabenfolgen zu entdecken. Wenn sich an dieser Aufgabe mehrere Personen beteiligen, sind bald viele solcher Folgen gefunden, wenn auch der erste Augenschein eher das Gegenteil vermuten läßt.

Hat man dann die Schlüsselwortlänge mit Hilfe von Kasiski–Abständen ermittelt, ist es sinnvoll, den verschlüsselten Text (nachträglich!) in Blöcke mit dieser Länge aufzuteilen. In unserem kurzen Beispiel mit der Schlüsselwortlänge 5:

```
OZRMY    PKMAL    DUMMY
OYIQE    OZRMK    OYIQE
CTLZA    MYVQX    SJX
```

Die Aufgabe, das am häufigsten auftretende Zeichen unter den ersten, den zweiten, ... Buchstaben in den Blöcken zu finden, sollte man wieder aufteilen. Besonders schnell kommt man voran, wenn eine Strichliste vorbereitet ist. Natürlich kann auch ein geeignetes Computerprogramm eingesetzt werden.

Das Entschlüsseln ist nach der Bestimmung des Codewortes kein Problem mehr. Da die Methode nur mit hinreichend langen Texten (oder wenig sinnvollen wie im Beispiel oben) tragfähig ist, ist diese Arbeit wieder aufzuteilen. Hilfreich ist dabei eine Alberti-Scheibe (s. o.). Empfehlenswert ist es auch, den zu entschlüsselnden Text mit größerem Zeilenabstand zu schreiben, damit die Lösung jeweils darüber oder darunter geschrieben werden kann.

Im Arbeitsbogen (Bild 10) finden Sie einen nach Vigenère verschlüsselten Text. Viel Spaß beim Entschlüsseln! Es handelt sich wieder um eine Denksportaufgabe. Wenn Sie einen eigenen Text verschlüsseln wollen, sollten Sie darauf achten, daß der Text – den Regeln des guten Stils entgegen – viele Wortwiederholungen enthält, um den Nachwuchskryptologen die Arbeit etwas zu vereinfachen. Weitere Materialien und Aufgaben zu den hier besprochenen Verfahren (u. a. eine Kopiervorlage zum Basteln einer Cäsar/Alberti-Scheibe) finden sich in dem Schülerarbeitsheft „Geheimschriften" (Beutelspacher, 1995), das besonders für die Sekundarstufe I geeignet ist.

Wenn Ihnen das Entschlüsseln nach Kasiski zu mühsam ist, können Sie auch das im LOG IN-Service erhältliche Programm verwenden, das eine (Roh-)Entschlüsselung mit dem Friedman-Test vornimmt, die sie dann interaktiv optimieren können. Dieses Programm können Sie auch verwenden, um bequem eigene Vigenère-chiffrierte Texte zu erzeugen. Im LOG IN-Service bekommen Sie (neben dem unten abgebildeten) auch einen zweiten Arbeitsbogen mit der Unterteilung des Textes in Blöcke der Länge 7 (= Schlüsselwortlänge) sowie einen dritten Bogen mit einer Strichliste zur Bestimmung des Schlüsselwortes.

Bild 10:
Geheimtext zur Dechiffrierung nach Kasiski.

Arbeitsbogen

Bestimmen der Schlüsselwortlänge

```
PWTMYTBADKDGPWPFYWFGUESOTLUPNVYWAPKCSO
OJWWASTLSUZUSJMJBBRSTIMGPYSXOJWWASMMZQ
LCHJQWGYDHKOJWWASTMFPADWIPVKLHONZWPDPW
RAAGQPRKNJCNPKGPJJLTHYOWOHPGYJWCUEKUZL
GAOWKHOGPESMZMRWPBKVFVZTQNLAGSFSMVWTDP
WRAAGQPRKNJCNPTGTKEOMSGVLYVCHKBVKLOFOB
LGNCIVXWPLYBZAAEOOWKEWEODZKZOGPWGOMSWM
PWTIFFLCTUTYGUOSLZSILYOHEWEODSRVVYHSFA
VVHHWGIPTGHYHCWJVLERGJWKPDHGJWTUTQNBXG
ZEUKTWIAZPPMOGPWGJQWGYDHKNJCNPSOVWTZPF
OMNQUQFGOWPYTQNBAIVOSXNSNZNVHMSPAHCXBW
VDTFJRWFLASXAGPHYHCWJVLEOANWKUPTXIYGUF
FSQLLHZRKZFGPYTXIYGUOWKVAEOEAOBBCVOSXV
WKUMSGVLYVCHKBOGYOSTSGGUYSTAAPKYWIPLBB
RSRIKULYJUVWKUPFHMDKLMWMMFRLCGUVKQSWAG
VVWYNVLZSILYROMKKJSBAZSWMOWKHMILSCKZAI
RPWZHMGPYSXLWTNCIVXWPIPNOMZGUSSXIMUIPY
UUEGUKICMDEOPFMZMRWPGOMYGOZSXBOKLGWKTW
HYLUKVEWZDAGVEKUOSYBWPZDHKTDGUFBJEWNJS
SLZSILYYUMFPAPAGVKVLWZKV
```

Die Vigenère-Verschlüsselung ist Teil der Unterrichtseinheit *Kryptologie* des neuen Berliner Rahmenplans für das Wahlpflichtfach Mathematik in der 10. Klasse. Falls Computer eingesetzt werden können, wird man im Mathematikunterricht eher fertige Programme verwenden. Im Informatikunterricht ist das natürlich anders.

Hinweise zur Programmierung im Informatikunterricht

Die Kryptologie bietet im Informatikunterricht viele Möglichkeiten für die Lernenden, Programme ganz unterschiedlichen Schwierigkeitsgrades selber zu erstellen (vgl. z. B. Sennholz, 1995; Künzell, 1998). Es ist sicherlich sinnvoll, in einer solchen Unterrichtseinheit auch Fragen des Datenschutzes, der Datensicherheit und der Kryptopolitik zu behandeln (vgl. Baumann, 1996, S. 374 ff.).

Um z. B. eine Cäsar-Chiffrierung zu programmieren, benötigt man als Sprachmittel (in der Terminologie der Wirthschen Sprachen PASCAL, MODULA und OBERON) lediglich die MOD-Funktion, ggf. Textdateien sowie eine Zuordnung zwischen Buchstaben und Zahlen (d. h. in der Regel den ASCII sowie die Funktionen ORD und CHR); für eine Tauschchiffre mit Schlüsselwort kommt noch der Datentyp ARRAY hinzu. Mit diesen Sprachmitteln kann man auch eine Vigenère-Verschlüsselung programmieren – all dies kann man also bereits im ersten Unterrichtsjahr Informatik realisieren.

Anspruchsvoller sind Programme zur Kryptoanalyse nach Kasiski oder Friedman. Im ersten Fall steht man vor der Alternative, Funktionen und Prozeduren aus einer Bibliothek zur Stringverarbeitung zu verwenden oder Algorithmen zur Mustersuche selbst zum Thema zu machen. Auch der Friedman-Test eignet sich hervorragend zur Programmierung, da eine Auswertung der Koinzidenzindizes „per Hand" schon bei geringer Zeichenzahl des Chiffrats sehr mühselig ist. Neben dem schon mehrfach erwähnten Programm aus dem LOG IN-Service gibt es auf der Begleit-CD zu dem Buch von Wobst (1997) C-Programme zur Bestimmung von Kappa aus Textdateien sowie zur Kryptoanalyse von Vigenère-Chiffren.

Wie geht es weiter?

Wie wir bereits weiter oben erwähnt haben, versagen der Kasiski- und der Friedman-Test, wenn man ein Schlüsselwort verwendet, das (mindestens) so lang ist wie der Klartext. Dies führt zu einer Chiffriermethode, die beweisbar(!) sicher ist und bei korrekter Anwendung nicht gebrochen werden kann. Leider hat diese Sicherheit auch ihren Preis, da das Verfahren kompliziert in der Anwendung ist, so daß die Kryptologen bislang noch nicht arbeitslos geworden sind ...

(Fortsetzung folgt)

StD Helmut Witten
Landesbildstelle Berlin
BICS
Wikingerufer 7
10555 Berlin
E-Mail: witten@bics.be.schule.de

OStR Irmgard Letzner
Fritz-Karsen-Schule
Onkel-Bräsig-Straße 76-78
12359 Berlin
E-Mail: letzner@math.fu-berlin.de

Prof. Dr. Ralph-Hardo Schulz
Freie Universität Berlin
Fachbereich Mathematik und Informatik
Institut für Mathematik II
Arnimallee 3
14195 Berlin
E-Mail: schulz@math.fu-berlin.de

Danksagung
Wir möchten Herrn Bänsch von der Bertha-von-Suttner-Oberschule (Gymnasium) in Berlin-Reinickendorf danken, daß er sein Programm zur Vigenère-Chiffrierung und -Dechiffrierung nach Friedman für den LOG IN-Service zur Verfügung gestellt hat.

(Im **LOG IN-Service** (s. S. 71) erhalten Sie dieses Programm (mit Turbo-PASCAL-Quellcode) zur Vigenère-Chiffrierung und -Dechiffrierung nach Friedman, das eine (Roh-)Entschlüsselung mit dem Friedman-Test vornimmt, die Sie dann interaktiv optimieren können. Dieses Programm können Sie auch verwenden, um bequem eigene Vigenère-chiffrierte Texte zu erzeugen. Des weiteren bekommen Sie (neben dem vorgestellten) auch einen zweiten Arbeitsbogen mit der Unterteilung des Textes in Blöcke der Länge 7 (= Schlüsselwortlänge) sowie einen dritten Bogen mit einer Strichliste zur Bestimmung des Schlüsselwortes.)

Literatur

Bauer, F. L.: Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie. Berlin u. a.: Springer, 1995.

Baumann, R.: Didaktik der Informatik (2., vollständig überarbeitete Auflage). Stuttgart u. a.: Klett-Verlag, 1996.

Beutelspacher, A.: Kryptologie – Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Braunschweig: Vieweg, ^{3}1993.

Beutelspacher, A.: Mathe-Welt – Geheimschriften. In: mathematik lehren, 13 (1995), H. 72, S. 23-46.

Beutelspacher, A.: Geheimsprachen – Geschichte und Techniken. München: Beck, 1997.

Kippenhahn, R.: Verschlüsselte Botschaften – Geheimschrift, Enigma und Chipkarte. Reinbek bei Hamburg: Rowohlt, 1997.

Kuenzell, St.: Binnendifferenzierung im Informatikunterricht. In: LOG IN, 18 (1998), H. 1, S. 51-55 (Teil 1: Voraussetzungen); H. 2, S. 51-55 (Teil 2: Unterrichtsplanung); H. 3/4, S. 77-82 (Teil 3: Unterrichtsverlauf); H. 5, S. 47-50, (Teil 4: Analysen und Tips).

Sennholz, K.: Verschlüsselte Botschaften. In: Informatik betrifft uns, 8 (1995), H. 2, S. 1-23.

Sgarro, A; Würmli, M.: Geheimschriften – Verschlüsseln und Enträtseln von Geheimtexten. Augsburg: Weltbild Verlag, 1991.

Witten, H.; Letzner, I.; Schulz, R.-H.: RSA & Co. in der Schule (Teil 1: Statistik und Sprache). In: LOG IN, 18 (1998), H. 3/4, S. 57-65.

Wobst, R.: Abenteuer Kryptologie – Methoden, Risiken und Nutzen der Datenverschlüsselung. Bonn u. a.: Addison-Wesley, 1997.