universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Einführung in die Kryptologie: von Cäsar bis RSA mit Übungsaufgaben

Eine Lehrunterlage für das Mathematik Wahlpflichtfach

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag. rer.nat.)

Verfasserin:	Marion Pilat
Matrikel-Nummer:	0306088
Studienrichtung (lt. Studien-blatt):	Lehramtsstudium: Unterrichtsfach Mathematik, Unterrichtsfach Biologie und Umweltkunde
Betreuer:	Mag. Dr. Andreas Ulovec

Wien, am 15.12.2008

Danksagung

Ich möchte mich hier bei den Menschen bedanken, die mich auf meinem bisherigen Weg begleitet haben: Ganz besonderer Dank gilt meinem Freund Werner für seine Liebe und Unterstützung, meinen Eltern, die mir das Studium und vieles andere in meinem Leben überhaupt ermöglicht haben, und meiner Oma, die mich schon immer motiviert hat und mir hilft, wo sie nur kann. Danke, dass ihr für mich da seid! Ich möchte mich außerdem bei allen Freunden und Studienkollegen bedanken, mit denen ich in den letzten Jahren viel Spaß hatte. Ein Dankeschön gebührt auch Professor Andreas Ulovec für seine verständnisvolle Betreuung.

Inhaltsverzeichnis

Kryptologie im Mathematik Wahlpflichtfach

Das Mathematik Wahlpflichtfach wird in vielen Schulen kaum angeboten oder selten von Schülern gewählt, weil im Mathematik Wahlpflichtfach oft nur noch einmal die Themen aus dem Regelunterricht, vielleicht etwas genauer und auf höherem mathematischen Niveau, durchgekaut werden. Das interessiert die Schüler meistens nicht.
Dass das Wahlpflichtfach leider oft nicht viel spannender für die Schüler als der Regelunterricht gestaltet werden kann, liegt vielleicht daran, dass es für Lehrer sehr schwierig ist, geeignete Themen und Unterlagen für ein Mathematik Wahlpflichtfach zu finden, da es eigentlich keine Lehrbücher gibt in denen man solche Unterlagen finden könnte. Das Thema Kryptologie eignet sich meiner Meinung nach sehr gut für das Wahlpflichtfach, da die Schüler vieles selbst erarbeiten, ausprobieren und entdecken können!

In meiner Diplomarbeit möchte ich das Thema Kryptologie so bearbeiten, dass sie als Unterlage für dieses Thema im Wahlpflichtfach verwendet werden kann.
Der Aufbau ist ähnlich wie in einem Lehrbuch. In jedem Kapitel gibt es zusätzlich zum Theorieteil meistens noch Wissenswertes, Historisches oder lustige Geschichten (kursiv geschrieben), außerdem einen Aufgabenteil (Angaben fett gedruckt), wobei zum Lösen der Aufgaben nur der Theorieteil notwendig ist. In einigen Kapiteln gibt es zusätzlich ein persönlicher Kommentar von mir, in dem ich z.B. didaktische Überlegungen oder Vorschläge äußere (gekennzeichnet durch einen Rahmen).
Die Arbeit soll aber nur als Unterlage für den Unterricht dienen, ist also kein genauer Unterrichtsvorschlag. Welche Kapitel eventuell weggelassen werden, die Reihenfolge der Kapitel, wie viel Zeit man den einzelnen Kapiteln widmet, welche Unterrichtsform man verwendet,… soll vom jeweiligen Lehrer selbst entschieden werden.

Alle Bezeichnungen wie Schüler, Lehrer,… sind geschlechtsneutral zu verstehen!

Einleitung

Wenn wir in der Geschichte zurückblicken, war es schon immer wichtig, dass Mitteilungen und Informationen nur an bestimmte Personen gelangten und gegenüber anderen geheim gehalten wurden.
Es gibt zwei Methoden, Nachrichten geheim zu übermitteln:
Die **Steganographie** ist die Wissenschaft der verborgenen Übermittlung von Informationen, d.h. die Existenz der Nachricht wird geheim gehalten. Das Wort kommt aus dem Altgriechischen *steganos* „schützend, bedeckt“ und *gráphein* „schreiben“, kann also als „verstecktes Schreiben“ übersetzt werden.
Hierbei wird z.B. mit unsichtbarer Tinte geschrieben oder es werden in einem unverfänglichen Text gewisse Buchstaben kaum merklich markiert.
Die **Kryptographie** ist die Wissenschaft von der Verschlüsselung von Informationen, hierbei versucht man nicht, die Existenz der Nachricht geheim zu halten. Der Sender verschlüsselt sie so, dass nur der Empfänger sie entschlüsseln und lesen kann. Der Name kommt aus dem Griechischen und setzt sich aus den Wörtern *kryptós*, „verborgen, geheim“, und *gráphein*, „schreiben“ zusammen.
Kryptologie besteht aus den beiden Teilgebieten Kryptographie und Kryptoanalyse, wobei die **Kryptoanalyse** ursprünglich die unbefugte Entzifferung von Geheimtexten bezeichnet, heutzutage beschäftigt sie sich aber allgemeiner mit der Analyse kryptographischer Verfahren (um sie entweder zu knacken oder ihre Sicherheit bzw. ihre Stärken und Schwächen nachzuweisen).
Während sich die Kryptologie früher hauptsächlich mit dem Erstellen und Lesen von Geheimschriften beschäftigte und somit ein Gebiet der Linguistik darstellte, ist sie heute ein Teil der angewandten Mathematik und für die Informationssicherheit von großer Bedeutung.

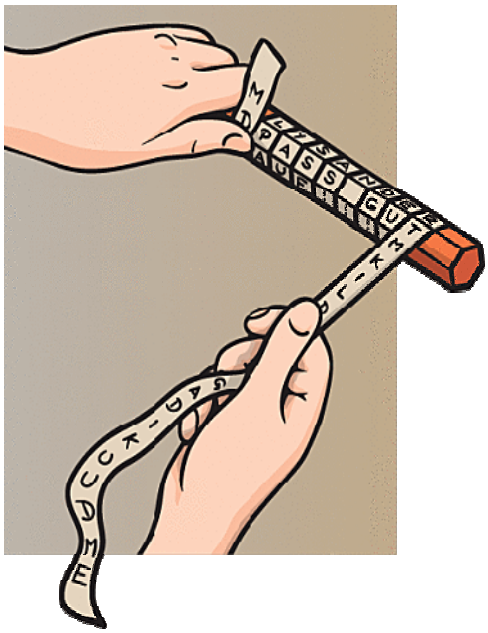
Begriffserklärung:
In der Kryptologie wird die zu übertragende Nachricht (oder Buchstaben- bzw. Zeichenfolge) als *Klartext* bezeichnet, die verschlüsselte Nachricht (oder Buchstaben- bzw. Zeichenfolge) nennt man *Geheimtext*.
Der Vorgang des Verschlüsselns heißt auch *Chiffrieren*, das Entschlüsseln *Dechiffrieren*. Die verwendete Chiffriermethode nennt man *Algorithmus* und als

Schlüssel wird die Information bezeichnet, die benötigt wird um den Klartext zu chiffrieren bzw. den Geheimtext zu dechiffrieren.
Das Entschlüsseln eines Geheimtextes ohne Kenntnis des Schlüssels wird als *brechen* bzw. als *knacken* bezeichnet.

1. Transpositionschiffren

1.1. Die Skytala von Sparta

Die älteste uns bekannte Methode der Kryptographie ist die Skytala von Sparta, ihre Geschichte beginnt vor etwa 2500 Jahren in Griechenland. Schon damals war es wichtig, Nachrichten auch geheim übermitteln zu können. Die Regierung benutzte die Skytala, um geheime Botschaften zu verschlüsseln und an ihre Generäle zu schicken. Diese mussten auch eine Skytala besitzen, um die Nachricht entschlüsseln zu können. Eine Skytala war ein Zylinder mit einem bestimmten Umfang, um den der Sender ein schmales Band aus Pergament oder Leder wickelte und dann der Länge nach die Nachricht darauf schrieb. Das Band wurde abgewickelt und konnte nur noch mithilfe einer Skytala gleichen Umfangs gelesen werden.



„Als den spartanischen Feldherrn Lysander im Jahre 404 v. Chr. ein völlig entkräfteter Bote aus Persien erreichte, nahm er ihm zuerst seinen Gürtel ab. Mit unzusammenhängenden Buchstaben versehen, hatte der Bote diesen bei seinem Aufbruch in Persien bekommen. Lysander zückte einen hölzernen Stab und wickelte den Gürtel sogleich darum. So erfuhr der Feldherr vom geplanten Angriff des Perserführers Pharnabasus. Dank der Skytala besiegte Lysander schließlich das persische Heer.“

Aus http://www.wissenschaft-online.de/artikel/914330

Die Skytalaverschlüsselung beruht darauf, dass man den Klartext in mehreren Zeilen (ihre Länge entspricht der Länge der Skytala) aufschreibt und den Geheimtext erhält, indem man diesen Text dann noch einmal spaltenweise aufschreibt.

Ein Bespiel:

„Welchen Umfang hatte diese Skytala“ wird zeilenweise aufgeschrieben:

W E L C H E

N U M F A N

G H A T T E

D I E S E S

K Y T A L A

und wird zu:

W N G D K E U H I Y L M A E T C F T S A H A T E L E N E S A

Der Schlüssel, mit dem man diese Botschaft dechiffrieren kann, ist die Anzahl der Zeilen. Diese entspricht dem Umfang u der Skytala, weil eine bestimmte Anzahl von Buchstaben um die Skytala herum passt. In diesem Fall ist u=5.

Besitzt man eine falsche, größere Skytala bzw. glaubt man der Schlüssel sei u=6, ergibt sich nur folgendes:

W U A S L

N H E A E

G I T H N

D Y C A E

K L F T S

E M T E A

Und das ergäbe als Klartext WUASLN…, also nur Unsinn.

Die Skytalaverschlüsselung ist eine **Transpositionschiffre**, das heißt, die Buchstaben werden in einer bestimmten Art und Weise vertauscht, wechseln also ihre Position. Sie werden aber nicht durch andere Zeichen oder Buchstaben ersetzt.

Aufgaben:

1. Welcher Klartext verbirgt sich hinter diesem mittels Skytala verschlüsselten Geheimtext?

I S A D T P I H E H N N C S D I R O O I L T H A I T A E A S N F E Z C S W E S S N I S F I U K T U J S E S T C R C K E !

Lösung:

Durch Ausprobieren erhält man u=12.

I C H W U
S S T E J
A D A S S
D I E S E
T R A N S
P O S I T
I O N S C
H I F F R
E L E I C
H T Z U K
N A C K E
N I S T !

Ich wusste ja dass diese Transpositionschiffre leicht zu knacken ist!

Oft erkennt man schon nach dem Aufschreiben der ersten Spalten, ob etwas Sinnvolles herauskommen kann.

z.B. bei u=4 erhält man

I T E C R …
S P H S O
A I N D O
D H N I I

und vermutet spätestens hier, dass man mit u=4 falsch liegt, da ITECR kein deutsches Wort bzw. einen Teil davon ergibt.

2. Bastelt selbst eine Skytala, schreibt eine Botschaft darauf und gebt den Gemheimtext eurem Tischnachbarn zum Entschlüsseln!

(Man kann eine Skytala aus Karton basteln oder auch anstelle eines Zylinders nur einen Streifen harten Karton benutzen. Auch Dosen oder leerer Küchenpapierrollen eignen sich gut.)

Lösung:
Bei den Botschaften sind der Kreativität der Schüler keine Grenzen gesetzt. Man kann die Botschaften auch einsammeln und zufällig verteilen. Wer eine Botschaft entschlüsselt hat, könnte diese vorlesen, u.s.w.

3. Wie groß ist ungefähr die Anzahl der möglichen Schlüssel bei der Skytalaverschlüsselung?

Lösung:
Bei der Verwendung einer echten Skytala ist die Anzahl der Schlüssel dadurch beschränkt, dass man sie nicht beliebig groß bauen kann, schon eine Skytala mit einem halben Meter Durchmesser dürfte relativ unpraktisch werden.
Außerdem ist die Anzahl der Schlüssel durch die Länge der Botschaft beschränkt. Sei n die Anzahl der Buchstaben des Klartextes. Man muss in eine Zeile mindestens 2 Buchstaben schreiben, sonst wird der Klartext nicht verschlüsselt, also kann u nicht gleich n sein. Außerdem muss u mindestens 2 sein, sonst bleibt der Text ebenfalls gleich. Bei einer geraden Buchstabenanzahl gibt es dann höchstens n/2 -1 mögliche Schlüssel, bei einer ungeraden Anzahl höchstens (n-1)/2.
Dies ist leicht mithilfe eines sehr kurzen Klartextes (8 oder 9 Buchstaben) zu überprüfen.

4. Oft bleiben bei einer Skytalaverschlüsselung mit u Zeilen am Ende einige Plätze leer.
1) Wann genau bleibt kein Platz leer?
2) Was passiert, wenn am Ende der Klartextes ein Satzzeichen steht, aber einige Plätze leer bleiben. Wo steht es dann im Geheimtext?
3) Wenn man die leeren Plätze mit lauter X auffüllt, wäre das gut oder wäre es ein Hinweis für einen Spion, der die Botschaft entschlüsseln will? Was gäbe es für Alternativen?

Lösung:
1) Sei n die Anzahl der Buchstaben des Klartextes. Es bleibt genau dann kein Platz leer, wenn u ein Teiler von n ist. Ist u ein Teiler von n, dann ist auch die Zeilenlänge (=Anzahl der Spalten) ein Teiler von n und umgekehrt.

2) Das Satzzeichen steht dann nicht mehr am Ende des Geheimtextes. Steht es an x-ter Stelle, muss u ein Teiler von x sein. Beim Entschlüsseln darf man in diesem Fall nach dem Satzzeichen nur noch (u-1) Zeilen anschreiben.
Steht also das Satzzeichen am Ende des Geheimtextes, weiß man dass kein Platz leer geblieben ist und somit u ein Teiler von n sein muss.
3) Die leeren Plätzen mit lauter X aufzufüllen wäre keine gute Idee. Da X eigentlich selten vorkommt, würde das Auffüllen mit X auch im Geheimtext sofort auffallen. Der Abstand zwischen diesen X, entspricht der Anzahl der Zeilen, also kennt man sofort den Schlüssel u.
Eine unauffälligere Möglichkeit wäre, die Plätze mit A B C D… aufzufüllen, da diese Buchstaben im Geheimtext weniger auffallen.
Noch besser wäre es, die Plätze mit irgendeinem (auch sinnlosen) Wort oder beliebigen (verschiedenen!) Buchstaben aufzufüllen.

5. Beispiele zur vorigen Aufgabe:

Zu 1) und 2)

ANEMDLENMELESEMENCNSMTHAEECWUEIHIF.

Lösung: Alle meine Entchen schwimmen auf dem See. (u=5)

A	L	L	E	M	E	I
N	E	E	N	T	C	H
E	N	S	C	H	W	I
M	M	E	N	A	U	F
D	E	M	S	E	E	.

Da die u ein Teiler von n ist, bleibt kein Platz leer. De Punkt steht auch im Geheimtext an letzter Stelle.

Zu 2)

NIAHSEHRIUNVASRAB.RBEITNFRERRIGEEE

Lösung: Nur ein braver Hai isst gerne Haferbrei. (u=9)

N U R E
I N B R
A V E R
H A I I
S S T G
E R N E
H A F E
R B R E
I .

Im Geheimtext steht der „.“ an der 18. Stelle. Also muss u ein Teiler von 18 sein, also 2, 6, 9 oder 18. Nach dem Punkt schreibt man nur noch u-1=8 Zeilen.

Zu 3)

KAV,IABRHOWCLEÄNRIHDNHUSRSV.TMIS

CEXDDETHRXERBDOLXREEUNIXHINDBEX

Lösung: Kräht der Hahn um drei vor sieben, wirst du dich schon bald verlieben. (u=7)

K R Ä H T D E R H
A H N U M D R E I
V O R S I E B E N
, W I R S T D U D
I C H S C H O N B
A L D V E R L I E
B E N . X X X X X

Der Abstand zwischen den X beträgt 7 Stellen, also muss u=7 sein.

6. Wie dechiffriert man eine Skytalaverschlüsselung, wenn u kein Teiler von n=Anzahl der Buchstaben des Geheimtextes ist (also einige Plätze leer bleiben), man aber nicht weiß, welches der letzte Buchstabe im Klartext war?

Lösung:

Ist u kein Teiler von n, dann gibt es $k = k_1+1$ Spalten, wobei $k_1= n : u + r_1$ (mit Rest) ist. Der Geheimtext wird in (k-r) Spalten der Länge u und r Spalten der Länge (u-1) geschrieben, wobei $r = u . k – n$ ist.

7. Einige Geheimbotschaften zum entschlüsseln:

WMLDEEEÜELRNSRLITSSSSSECTTCLHEIHNN?

Lösung: Wer ist im Entschlüsseln der Schnellste? (u=5)

W E R I S T I
M E N T S C H
L Ü S S E L N
D E R S C H N
E L L S T E ?

MASASSCEEHNLTTNESSUCPCHAHLßDÜ?

Lösung: Macht euch das Entschlüsseln Spaß? (u=3)

M A C H T E U C H D
A S E N T S C H L Ü
S S E L N S P A ß ?

Kommentar:

Bei dieser relativ einfachen und auch leicht zu knackenden Verschlüsselungsmethode macht es den Schülern wahrscheinlich Spaß, sich irgendwelche lustigen Geheimbotschaften zu schicken. So ist das ein spielerischer Einstieg ins Thema Kryptologie.

1.2. Weitere einfache Transpositionschiffren

Krebs

Krebs ist ein sehr einfaches Verschlüsselungsverfahren: Die Nachricht wird wortweise oder im Ganzen rückwärts gelesen.

Ein Beispiel:

DAS IST GEHEIM wird zu

SAD TSI MIEHEG oder zu

MIEHEG TSI SAD.

Palindrome sind Wörter oder sogar ganze Sätze, die durch Krebs nicht verändert werden, d.h. vorwärts und rückwärts gelesen gleich bleiben.

Beispiele:

Reliefpfeiler, Lagerregal, Reittier, Marktkram, Otto, Rentner,…

Oh Chello voll Echo

O Genie, der Herr ehre Dein Ego!

Trug Tim eine so helle Hose nie mit Gurt?

Nur du Gudrun

Eine güldne, gute Tugend: Lüge nie!

A man, a plan, a canal: panama

Madam, i´m Adam

Was it a cat I saw?

Würfel

Der Klartext wird in ein Rechteck einer bestimmten Zeilenlänge k geschrieben:

Zum Beispiel: k=7

d e r w ü r f

e l h a t i m

m e r s e c h

s s e i t e n

Wird der Text nun spaltenweise gelesen, ergibt sich die Skytalaverschlüsselung:

D E M S E L E S R H R E W A S I Ü T E T R I C E F M H N

Es gibt aber noch viele andere Möglichkeiten:

- Schlangenwürfel: spaltenweise, aber einmal von oben, einmal von unten lesen

  D E M S S E L E R H R E I S A W Ü T E T E C I R F M H N

- Diagonalwürfel: diagonal gelesen:

  S M S E E E D L R I E H S T R A E E W T C N Ü I H R M F

- Schneckenwürfel: in einer Spirale gelesen:

  F R Ü W R E D E M S S E I T E N H M I T A H L E R S E C

- usw.

Gartenzaunchiffre

Anstelle eines Rechtecks können auch andere geometrische Formen verwendet werden, zum Beispiel die „Gartenzaumform“:

D S N T A
A I T I G R E Z U
S E A N N

wird zeilenweise gelesen zu D S N T A A I T I G R E Z U S E A N N

Aufgaben:

1. Überlege dir eine besonders schwierige Würfelverschlüsselung?

Lösung:

Hier ist wieder Kreativität gefragt, es kann bestimmtes Muster sein, oder man kann auch die Stellen des Würfels irgendwie nummerieren und dann die Buchstaben in dieser Reihenfolge abschreiben. Hauptsache, alle Buchstaben finden sich dann auch im Geheimtext wieder!

2. Überlege dir eine andere geometrische Form, als den Gartenzaun!

Lösung:

Ein Beispiel sind Rauten oder Kreuze:

b f j n r v y
a c e g i k m o q s u w z
d h l p t x !

a g m s
b c d h i j n o p t u v
e k q w
f l r x

Um die Botschaft zu verschlüsseln wird wieder zeilenweise gelesen.

***Kommentar*:**

In diesem Kapitel muss nicht unbedingt alles gleich “verraten“ werden, viel spannender für die Schüler (und auch für den Lehrer) ist es, zu sehen welche Möglichkeiten die Schüler selbst entdecken. Man könnte auch gleich fragen, ob den Schülern bei der Skytalaverschlüsselung etwas anderes einfällt als spaltenweises Ablesen.

Oder vielleicht fragt gleich ein Schüler nach: „Warum kann man das denn nicht genauso gut von unten nach oben ablesen?“ Hier ist es sicher wichtig, keine Schülerfragen abzublocken, sondern Fragen und Diskussionen zu fördern! Das Thema ist nämlich hervorragend dafür geeignet, die Schüler selbstständig entdecken, herausfinden, überlegen, ausprobieren,… zu lassen.

1.3. Spaltentransposition

1.3.1. Einfache Spaltentransposition

Die Spaltentransposition ähnelt der Skytalaverschlüsselung. Man schreibt die Nachricht in Zeilen mit einer bestimmten Länge k. Bevor man spaltenweise abliest, werden die Spalten aber noch mithilfe einer vorgegeben Permutation π vertauscht. Der Schlüssel ist also k und π.

Definition:

Eine Permutation ist eine Veränderung der Reihenfolge von Elementen einer Menge, d.h. sie ist eine eineindeutige Abbildung einer Menge auf sich selbst.

Ein Beispiel:

Vertrauen ist gut k=5 π: 21543

Der Text wird nun also in Zeilen der Länge 5 geschrieben. Die Spalten werden mit 1 2 3 4 5 nummeriert und dann so vertauscht dass sie in der Reihenfolge 2 1 5 4 3 stehen. (Somit steht dann zuerst die 2., dann die 1., 5., 4. und zuletzt die 3. Spalte.)

1 2 3 4 5	*2 1 5 4 3*
v e r t r	E V R T R
a u e n i	U A I N E
s t g u t	T S T U G

Nun wird spaltenweise abgelesen:
E U T V A S R I T T N U R E G

(Man könnte auch zeilenweise ablesen:
E V T R T R U A I N E T S T U G
Kurze Wörter werden dabei aber oft nur wenig verändert und sind manchmal auf den ersten Blick leicht zu entschlüsseln, hier z.B. am Ende des Geheimtextes gut wird nur zu TUG.)

Beim Entschlüsseln geht man genau umgekehrt vor: Man schreibt den Geheimtext spaltenweise, nummeriert die Spalten mittels π: 21543 ordnet sie in der Reihenfolge 12345 und liest zeilenweise.

1.3.2. Gemischte Zeilen- Spalten- Transposition

Die gemischte Zeilen- Spalten- Transposition funktioniert in Prinzip wie die einfache Spaltentransposition, arbeitet aber mit einer zusätzlichen Zeilenpermutation.
Die Nachricht wird zeilenweise aufgeschrieben und die Zeilen werden mithilfe einer Permutation π_1 umgeordnet. Anschließend werden die Spalten mittels einer Permutation π_2 umgeordnet, dann wird spaltenweise abgelesen.
(Es kann hier auch wie bei der einfachen Spaltentransposition zeilenweise abgelesen werden, dies wird dann als gemischte Zeilen- Block- Transposition bezeichnet.)

Ein Beispiel:
Kontrolle ist besser k=6 π_1: 321 π_2: 524613

Die Zeilen werden mit 1 2 3 nummeriert und dann in der Reihenfolge 3 2 1 angeschrieben. Dann wie vorher die Spalten mit 1 2 3 4 5 nummeriert und in der Reihenfolge 5 2 4 6 1 3 geschrieben.

							1	*2*	*3*	*4*	*5*	*6*		*5*	*2*	*4*	*6*	*1*	*3*
1	k	o	n	t	r	o	*3*	b	e	s	s	e	r	E	E	S	R	B	S
2	l	l	e	i	s	t	2	l	l	e	i	s	t	S	L	I	T	L	E
3	b	e	s	s	e	r	*1*	k	o	n	t	r	o	R	O	T	O	K	N

Ergibt spaltenweise gelesen:
E E S R B S S L I T L E R O T O K N

Die Entschlüsselung funktioniert wie bei der einfachen Spaltentransposition indem man in umgekehrter Richtung vorgeht.

1.3.3. Doppelte Spaltentransposition

Im 1. und sogar noch im 2.Weltkrieg wurde die doppelte Spaltentransposition benutzt, wobei zweimal hintereinander eine Spaltentransposition mit dem gleichen oder verschiedenem Schlüssel durchgeführt wurde. Die doppelte Spaltentransposition wurde aber meistens vom jeweiligen Gegner gebrochen.

Aufgaben:

1. Verschlüssle eine Nachricht mittels Spaltentransposition (einfache oder gemischte) und gebe sie (inklusive Schlüssel, also k und π)deinem Tischnachbarn zum entschlüsseln!

2. Was passiert, wenn man bei der gemischten Zeilen- Spalten- Transposition zuerst π_2 und dann π_1 anwendet? Überprüfe deine Vermutung anhand eines Beispiels!

Lösung:
Wendet man zuerst π_2 auf die Spalten und dann π_1 auf die Zeilen an, entsteht genau der gleiche Geheimtext. π_2 bleibt dabei die Spaltenpermutation und π_1 die Zeilenpermutation. Zur Überprüfung kann man das Beispiel von vorhin („Kontrolle ist besser“ verwenden).

Kommentar:

Man muss natürlich im Wahlpflichtfach nicht alle Transpositionschiffren durchmachen. Es kommt darauf an, wie viel Zeit man zur Verfügung hat und wie viel Spaß diese einfachen Chiffriermethoden den Schülern machen!

Zusammenfassung Transpositionschiffren:

Die Buchstaben des Klartextes werden in einer bestimmten Art und Weise vertauscht, sie wechseln also ihre Position. (Eine Transpositionschiffre ist eine Permutation der Stellen des Klartextes.)

Skytalaverschlüsselung

Schlüssel: u= Umfang der Skytala (gemessen in Buchstaben) bzw. Anzahl der Zeilen

Chiffrieren: Der Klartext wird zeilenweise geschrieben, dabei ergeben sich genau u Zeilen. Man erhält den Geheimtext, indem man den Text spaltenweise liest.

Dechiffrieren: Der Geheimtext wird spaltenweise mit genau u Zeilen aufgeschrieben. Man erhält den Klartext, indem man zeilenweise liest.

Würfel

Schlüssel: Zeilenlänge k und der Weg nach dem abgelesen wird

Chiffrieren: Der Klartext wird zeilenweise in Zeilen der Länge k geschrieben. Man erhält den Geheimtext, indem man den Text nach einem bestimmten Weg abliest.

Dechiffrieren: Der Geheimtext wird im gleichen Weg aufgeschrieben und der Klartext zeilenweise abgelesen.

Gartenzaunchiffre

Schlüssel: Eine bestimmte geometrische Form (z.B. Gartenzaun)

Chiffrieren: Der Klartext wird in einer bestimmten Form aufgeschrieben und der Geheimtext zeilenweise abgelesen.

Dechiffrieren: Der Geheimtext wird zeilenweise in eine bestimmte Form geschrieben und der Klartext der Form nach abgelesen.

Spaltentransposition

Schlüssel: Zeilenlänge k und Permutation π

Chiffrieren: Der Klartext wird in Zeilen der Länge k geschrieben. Die entstandenen Spalten werden mittels π vertauscht und der Geheimtext wird spaltenweise abgelesen.

Dechiffrieren: Man schreibt den Geheimtext spaltenweise, nummeriert die Spalten mittels π ordnet sie in richtiger Reihenfolge und liest den Klartext zeilenweise.

2. Substitutionschiffren

Die Buchstaben des Klartextes behalten ihre Position, werden aber durch einen anderen Buchstaben oder ein anderes Zeichen ersetzt.

2.1. Monoalphabetische Chiffren

Bei monoalphabetischen Chiffren wird ein Klartextbuchstabe immer durch den gleichen Geheimtextbuchstaben (oder –zeichen) ersetzt.

2.1.1. Verschiebechiffren oder „Cäsar-Verschlüsselung“

Der römische Feldherr Julius Cäsar (100 bis 44 v.Chr.) soll auch schon kryptologische Techniken zur geheimen Kommunikation verwendet haben. Unter anderem benutzte er eine Verschiebechiffre: Cäsar ersetzte jeden Buchstaben des Klartextes durch den Buchstaben, der 3 Stellen weiter im Alphabet steht.

Der römische Schriftsteller Sueton beschreibt das Verfahren wie folgt (aus C. Suetonius Tranquillus, De Vita Caesarum, LVI):

> *„… si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.“*

> *„… wenn etwas Geheimes zu überbringen war, schrieb er in Zeichen, das heißt, er ordnete die Buchstaben so, dass kein Wort gelesen werden konnte: Um diese zu lesen, tauscht man den vierten Buchstaben, also D für A aus und ebenso mit den restlichen.“*

Deshalb wird diese Form der Substitution heute oft einfach als Cäsar-Verschlüsselung bezeichnet.

Die von Cäsar benutzte Chiffre erhält man, indem man unter das Klartextalphabet das Geheimtextalphabet - um 3 Stellen nach links verschoben – schreibt:

```
Klartextalphabet:     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
Geheimtextalphabet:   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
```

Chiffriert wird, indem man jeden Klartextbuchstaben durch den darunter stehenden Geheimtextbuchstaben ersetzt. Beim Dechiffrieren ersetzt man einfach jeden Geheimtextbuchstaben durch den darüberstehenden Klartextbuchstaben.
Zum Beispiel:
„veni vidi vici“ wird zu „YHQL, YLGL, YLFL“

Nun kann man natürlich nicht nur diese Cäsar- Verschiebung um drei Stellen verwenden, sondern kann mit Verschiebung zwischen einer und 25 Stellen insgesamt 25 verschiedene Geheimtexte erzeugen. (Bei Verschiebung um 26 Stellen gelangt man wieder zum ursprünglichen Klartextalphabet.)
Der Schlüssel ist hierbei die Anzahl der Stellen, um die verschoben wurde.

Eine Übersicht über alle 25 Verschiebechiffren:

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

Aber auch mit dieser Tabelle ist es relativ mühsam, einen längeren Text zu verschlüsseln. Mit einer Chiffrierscheibe kann man alle Verschiebechiffren schnell einstellen. Sie besteht aus zwei Scheiben, auf deren Rand jeweils das Alphabet in natürlicher Reihenfolge geschrieben ist. Die Scheiben sind im Mittelpunkt beweglich aneinander befestigt, sodass man sie gegeneinander verdrehen kann. Hat man die Scheibe richtig eingestellt (so dass das innere Alphabet um die richtige Anzahl an Stellen gegenüber dem äußeren verschoben ist) bedeutet Chiffrieren einfach Lesen von außen nach innen und Dechiffrieren bedeutet Lesen von innen nach außen. Die abgebildete Chiffrierscheibe ist auf die Verschiebung +3 eingestellt.

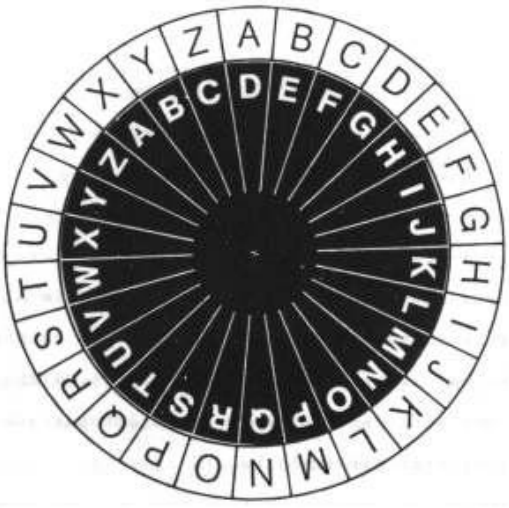
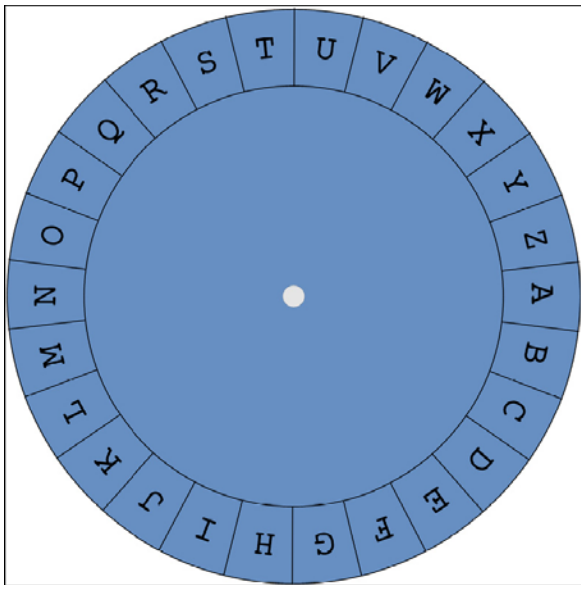
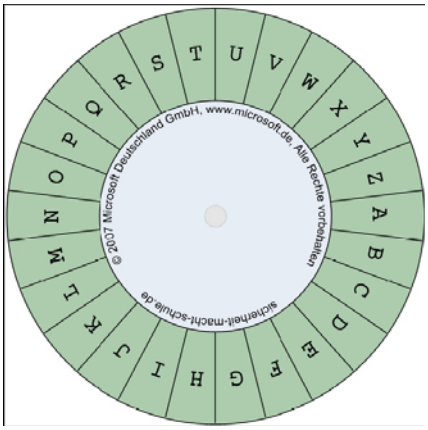


Abb. aus H.W.Franke: Die geheime Nachricht

„Cäsars Chiffrierscheibe – Anleitung zum Selbstbauen
Man druckt sich am besten das Blatt auf etwas dickerem Papier aus. Nun schneidet man die beiden Scheiben vorsichtig aus. Dann legt man die kleinere Scheibe auf die größere und befestigt die beiden Scheiben mit einer Klammer. Und schon kann man den gewünschte Verschiebefaktor einstellen und Texte verschlüsseln oder entschlüsseln.“





Aus http://www.sicherheit-macht-schule.de/media/pdf/563.pdf

Verschiebchiffre mit Zahlen

Ersetzt man jeden Buchstaben des Klartextalphabets durch eine Zahl, also A durch 1, B durch 2, C durch 3,… und Z durch 26, dann ist eine Verschiebechiffre einfach die Addition einer fixen Zahl. (Deshalb nennt man Verschiebechiffren auch manchmal **additive Chiffren**.)

Die oben beschriebene „Cäsar- Verschlüsselung“, wobei a durch D ersetzt wurde, entspricht der Addition der Zahl 3.

Dabei muss beachtet werden, dass nach 26 wieder bei 1 weitergezählt werden muss, d.h. in unserem Fall 25+3=2, also y wird zu B. Dabei rechnet man (25+3) **modulo** 26, wobei man den Rest der bei der Division durch 26 bleibt, erhält. (25+3) mod 26 = 28 mod 26 = 2, weil 28:26 =1 und 2 Rest (man schreibt auch 28=1.26+2).

Will man B wieder dechiffrieren, rechnet man (2-3) mod 26 = -1 mod 26 = 25, weil -1 = -1.26 + 25. und das entspricht dem Klartextbuchstaben y.

Aufgaben:

1. Bastelt eine Chiffrierscheibe!

2. Chiffriert eine Nachricht mit einer beliebigen „Cäsar- Verschlüsselung“ und gebt sie eurem Tischnachbarn zum Entschlüsseln! Verratet auch gleich den Schlüssel!

3. Wenn man weiß, dass ein Text mittels Verschiebechiffre verschlüsselt wurde, man aber den Schlüssel nicht kennt, kann man den Geheimtext knacken? Wie viele Versuche braucht man höchstens?

Lösung:

Da es nur insgesamt 25 mögliche Verschiebchiffren gibt, kann der Geheimtext relativ leicht geknackt werden, indem man einfach alle 25 möglichen Schlüssel ausprobiert (d.h. man benötigt höchstens 25 Versuche).

Die Verschiebechiffre ist also kein sehr guter Algorithmus, da sie leicht zu brechen ist.

4. Berechne:

7 mod 26

30 mod 26

36 mod 26

80 mod 26

26 mod 26

Welchen Buchstaben im Alphabet entsprechen die Ergebnisse?

Lösung:

7mod26 =7, weil 7=0.26 + 7, entspricht G

30mod26 = 4, weil 30=1.26 + 4, entspricht D

36mod26 = 10, weil 36=1.26 + 10, entspricht J

80mod26 = 2, weil 80=3.26 + 2, entspricht B

26mod26 = 26, weil 26=0.26 + 26, entspricht Z

2.1.2. Multiplikative Chiffren

Analog zur Verschiebechiffre (=additive Chiffre), bei der eine feste Zahl t zum Wert der Klartextbuchstaben addiert wird, kann man die Werte der Klartextbuchstaben auch mit einer Zahl s multiplizieren.

Man ersetzt die Klartextbuchstaben wieder durch die Zahlen 1 bis 26, multipliziert mit einer Zahl s und der Geheimtextbuchstabe entspricht dem Rest bei der Division durch 26.

Multipliziert man den Wert der Klartextbuchstaben mit 2 erhält man:

Klartextalphabet:	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
Geheimtextalphabet:	B	D	F	H	J	L	N	P	R	T	V	X	Z	B	D	F	H	J	L	N	P	R	T	V	X	Z

Hier werden aber verschiedene Klartextbuchstaben auf gleiche Geheimtextbuchstaben abgebildet, z.B. a und n auf B, b und o auf D, u.s.w.

Der Geheimtext soll aber eindeutig mithilfe des Schlüssels dechiffriert werden können. Also ist diese Substitution als Chiffre nicht geeignet.

Multipliziert man den Wert der Klartextbuchstaben mit 3 erhält man:

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

Diesmal erhalten wir im Geheimtextalphabet keine mehrfach vorkommenden Buchstaben, also ist diese Substitution als Multiplikative Chiffre geeignet.

Aufgaben:

1. Für welche Zahlen s ergibt sich durch Multiplikation mit s eine multiplikative Chiffre? Wie viele multiplikative Chiffren gibt es also?

Lösung:
Eine Multiplikation mit s ergibt genau dann eine Chiffrierung, wenn s und 26 teilerfremd sind. Das sind 1,3,5,7,9,11,15,17,19,21,23,25. (Bei s=1 wird der Text nicht verschlüsselt.)
Also gibt es 11 multiplikative Chiffren.

2. Verschlüssle einen beliebigen Klartext mit einer multiplikativen Chiffre!

3. Wie sicher ist eine multiplikative Chiffre?

Lösung:
Nicht sehr sicher: Zum knacken des Geheimtextes muss man nur 10 mögliche Schlüssel ausprobieren. (Der Schlüssel s=1 ist dabei natürlich nicht mitgezählt.)

2.1.3. Tauschchiffren oder affine Chiffren

Die multiplikative Chiffre ist mit nur 11 möglichen Schlüsseln noch unsicherer als die Verschiebchiffre. Man kann aber die multiplikativen und additiven Chiffren kombinieren und so die Sicherheit erhöhen.
Der Schlüssel einer Tauschchiffre besteht aus einem Zahlenpaar (s,t). Der Wert eines Klartextbuchstabens wird zuerst mit s multipliziert (dabei muss s wie oben teilerfremd zu 26 sein) und dann wird t addiert. Der Wert des Geheimtextbuchstaben entspricht wieder dem Rest bei Division durch 26.

Ein Beispiel:
hallo entspricht 8-1-12-12-15, mit dem Schlüssel (3,7) erhalten wir:
3.8+7mod26 = 31mod26 = 5
3.1+7mod26 = 10mod26 = 10
3.12+7mod26 = 43mod26 = 17
3.12+7mod26 = 43mod26 = 17
3.15+7mod26 = 52mod26 = 0
Also den Geheimtext 5-10-17-17-0 und das entspricht EJQQZ

Um den Geheimtext zu dechiffrieren muss man zuerst die Zahl s' berechnen, wobei s.s'mod26 = 1.
Alle Möglichkeiten für s und s':
s: 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
s': 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25
Es wird vom Wert des Geheimtextbuchstabens t subtrahiert und dann mit s' multipliziert. Der Rest bei Division durch 26 entspricht dem Klartextbuchstaben.

Beispiel von oben:
s=3, t=7 => s'=9
E entspricht 5, also (5-7).9mod26 = -18mod26 = 8, also h
J entspricht 10, also (10-7).9mod26 = 27mod26 = 1, also a
Q entspricht 17, also (17-7).9mod26 = 90mod26 = 12, also l
Q entspricht 17, also (17-7).9mod26 = 90mod26 = 12, also l
Z entspricht 0, also (0-7).9mod26 = -63mod26 = 15, also o

Aufgaben:

1. Verschlüssle einen Text mithilfe einer Tauschchiffre!

2. Wie viele mögliche Schlüssel gibt es bei Tauschchiffren?

Lösung:
Alle Schlüssel bestehen aus einem Zahlenpaar (s,t), wobei es für s genau 12 und für t genau 26 Möglichkeiten gibt: s aus {1,3,5,7,9,11,15,17,19,21,23,25} und t zwischen 0 und 25.
(Bei s=1 ergibt sich allerdings eine rein additive Chiffre, bei t=0 eine rein multiplikative Chiffre, bei s=1 und t=0 wird der Text somit gar nicht verschlüsselt.)
Also gibt es insgesamt 12.26 mögliche Zahlenpaare, d.h. 312 verschiedene Schlüssel.

3. Entschlüssle den folgenden Text mit dem Schlüssel (11,20):
LORSW, LOW QRU DWQFW WORHEAD QRL WORVWQADFWRL WJUADWORWR, MOW WFME LOW EJF, LOW TEDVWR TQ UADJWOPWR, GOF ODJWG UFWVVWRMWJFUIUFWG QRL LWJ WORHQWDJQRS WORWU UIGPCVU HQWDJ RQVV, LEU LWG SERTWR WJUF LOW BCVVWRLQRS SEP, WJHCJLWJFWR TQ ODJWJ WJHORLQRS QRSVEQPVOADW GQWDW. UWVPUF RCAD WORHEADWJW LORSW, LOW LWR KWJR LWU GEFDWGEFOUADWR LWRKWRU POVLWR, LOW EPUFJEKFDWOF QRL EVVSWGWORSQWVFOSKWOF LWJ TEDV GQUUFWR WJUF OR ZEDJWVERSWR PWGQWDQRSWR WJJQRSWR MWJLWR.

Lösung:

Klartextbuchstabe	Klartextzahl	Geheimtextzahl	Geheimtextbuchstabe
A	1	11.1+20mod26=5	E
B	2	11.2+20mod26=16	P
C	3	11.3+20mod26=1	A
D	4	11.4+20mod26=12	L
E	5	11.5+20mod26=23	W
F	6	11.6+20mod26=8	H
G	7	11.7+20mod26=19	S
H	8	11.8+20mod26=4	D
I	9	11.9+20mod26=15	O
J	10	11.10+20mod26=26	Z
K	11	11.11+20mod26=11	K
L	12	11.12+20mod26=22	V
M	13	11.13+20mod26=7	G
N	14	11.14+20mod26=18	R
O	15	11.15+20mod26=3	C
P	16	11.16+20mod26=14	N
Q	17	11.17+20mod26=25	Y
R	18	11.18+20mod26=10	J
S	19	11.19+20mod26=21	U
T	20	11.20+20mod26=6	F
U	21	11.21+20mod26=17	Q
V	22	11.22+20mod26=2	B
W	23	11.23+20mod26=13	M
X	24	11.24+20mod26=24	X
Y	25	11.25+20mod26=9	I
Z	26	11.26+20mod26=20	T

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

Der Klartext lautet:
Dinge, die uns heute einfach und einleuchtend erscheinen, wie etwa die Art, die Zahlen zu schreiben, mit Ihrem 'Stellenwertsystem' und der Einführung eines Symbols für Null, das dem Ganzen erst die Vollendung gab, erforderten zu ihrer Erfindung unglaubliche Mühe.
Selbst noch einfachere Dinge, die den Kern des mathematischen Denkens bilden, die Abstraktheit und Allgemeingültigkeit der Zahl, mussten erst in jahrelangen Bemühungen errungen werden.
Aus http://www.zahlenjagd.at/artikel97.html

2.1.4. Weitere einfache monoalphabetische Chiffren

Bei einer monoalphabetischen Chiffre kann das Geheimtextalphabet aus beliebigen Zeichen bestehen. Der Geheimtext muss nur mithilfe des Schlüssels eindeutig dechiffriert werden können.
Zum Beispiel:

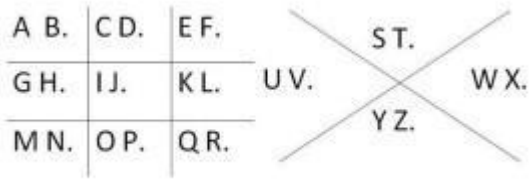
Klartextalphabet:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet	⇆	↓↑	↹	↓↑	⇇	⇉	⇈	⇊	∩	∪	↳	↰	↻	↺	⍉	⍲	⍱	⍳	␣	␣	⇪	⇪	⇦	↳	⇄	↹

Soll der Geheimtext wieder aus den Buchstaben des Alphabets bestehen, dann ist das Geheimtextalphabet eine beliebige Umordnung (=Permutation) des Klartextalphabets.
Zum Beispiel:

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

Es gibt zwar sehr viele Möglichkeiten das Alphabet umzuordnen, nämlich 26! (das sind über 400 000 000 000 000 000 000 000 000 Möglichkeiten), aber wie in den letzten beiden Beispielen ist der Schlüssel oft schwierig zu merken und er kann auch nicht leicht geheim übertragen werden, da er aus dem gesamten Geheimtextalphabet besteht.

Ein Beispiel für eine einfache monoalphabetische Substitution, die mit Symbolen im Geheimtextalphabet arbeitet, ist die **Freimaurerchiffre**:

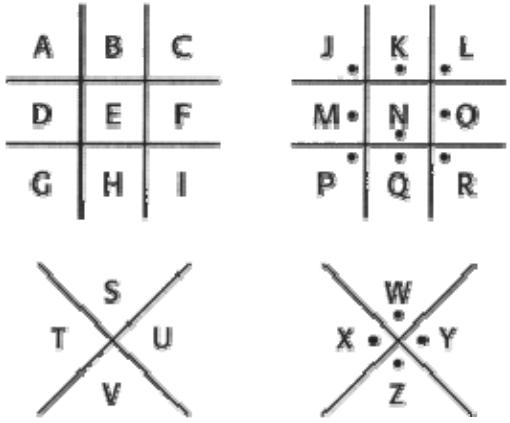


Aus http://martin-moeller.jimdo.com/krypto_-_freimaurerchiffre.php

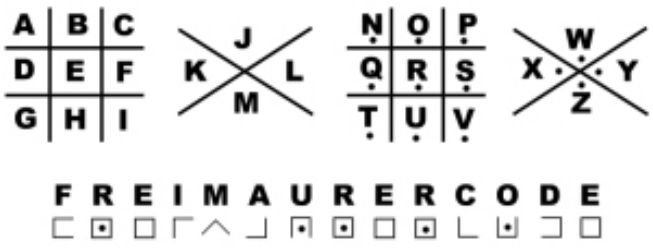
Die Buchstaben werden gemäß dem obigen Raster ersetzt:

F R E I M A U R E R – C H I F F R E wird zu

Es gibt allerdings einige verschiedene Varianten der Freimaurerchiffre, z.B. diese hier:



Aus http://www.gat-blankenburg.de/pages/fach/info/frei.htm



Aus http://www.code-knacker.de/verschluesselung.htm

Aufgaben:

1. Erfinde eine beliebige Substitutionschiffre. Verschlüssle einen Text mithilfe deiner Chiffre! Kann man sich das Geheimtextalphabet leicht merken?

2.1.5. Schlüsselwortchiffre

Eine weitere Möglichkeit der Substitution mit vielen Schlüsseln, aber einfach zu merkendem Geheimtextalphabet, ist die Schlüsselwortchiffre.
Der Vorteil besteht darin, dass man sich nicht das gesamte Geheimtextalphabet merken muss, sondern nur ein Schlüsselwort.
Man erzeugt das Geheimtextalphabet, indem man das Schlüsselwort ohne Buchstabenwiederholung aufschreibt und dann die restlichen Buchstaben des Alphabets, die noch nicht im Schlüsselwort vorgekommen sind, aufschreibt.

Ein Beispiel:
Als Schlüsselwort nehmen wir SUBSTITUTION
Also lautet das Geheimtextalphabet:

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

Um zu vermeiden, dass die letzten Buchstaben im Klartextalphabet nicht verschlüsselt werden, ist es noch besser, neben dem Schlüsselwort noch einen Schlüsselbuchstaben zu verwenden. Das Schlüsselwort steht dann nicht unter dem „a“ im Klartextalphabet, sondern unter dem Schlüsselbuchstaben. Nach dem Schlüsselwort wird wieder mit dem restlichen Alphabet „aufgefüllt“.

Ein Beispiel:
Schlüsselwort SUBSTITUTION und Schlüsselbuchstabe „f“

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

Noch eine andere Möglichkeit besteht darin, nach dem letzten Buchstaben des Schlüsselwortes das restliche Alphabet nicht mit A zu beginnen, sondern mit dem auf den letzten Schlüsselwortbuchstaben folgenden Buchstaben des Alphabets.
So kann auch ohne Schlüsselbuchstaben vermieden werden, dass die letzten Buchstaben des Klartextalphabets eventuell nicht verschlüsselt werden.

Ein Beispiel:

Schlüsselwort SUBSTITUTION

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

Auf den letzten Buchstaben des Schlüsselworts, nämlich N, folgt P (da das O schon im Schlüsselwort selbst vorkommt).

Dieses Verfahren galt dank der riesigen Anzahl an möglichen Schlüssel sehr lange (bis Ende des 1.Jahrtausends) als unüberwindbar. Lange Zeit bewahrheitete sich diese Annahme und deshalb war die monoalphabetische Substitution über Jahrhunderte gebräuchlich.

Aufgaben:

1. Verschlüssle einen Text mithilfe einer Schlüsselwortchiffre!

2. Dechiffriere den folgenden Text mit dem Schlüsselwort „Schnecke“ und Schlüsselbuchstabe „n“:
PVQ KOUSQOXQS TQUQS SVQZLYK LBK PQSS FC KVQ KVSP VKA LBOU VUE ULBK

Lösung:

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

Die Schnecken gehen niemals aus denn wo sie sind ist auch ihr Haus

3. Überlege dir ein Schlüsselwort, das auch noch nach dem Weglassen der schon vorgekommenen Buchstaben besonders lang ist! Wer findet das längste Schlüsselwort?

Wissenswertes:
Ein Wort, das alle Buchstaben gleich oft (also im einfachsten Fall genau einmal) enthält, wird als ***Isogramm*** *bezeichnet. Die längsten deutschen Isogramme ohne Sonderbuchstaben (also ohne Umlaute und ß), die auch tatsächlich manchmal verwendet werden, sind Fachbildungsprojekt (19 Buchstaben) und Dialogschwerpunkt (17 Buchstaben). Das längste wirklich gebräuchliche deutsche Isogramm ist Dialektforschung (16 Buchstaben) und auch Polschraubzwinge (16Buchstaben). Isogramme mit 15 Buchstaben gibt es schon mehr: unproblematisch, Bildungsprojekt, Zwischenprodukt, Komplizenschaft,…*
Darüber hinaus gibt es noch längere deutsche Isogramme, die allerdings Fantasiewörter sind: Jagdkniestrumpfloch (19), Wildbachverstopfung (19), Zylinderkopfwachstum (20), Konvexrumpfschwitzbad (21) und oxydschmelzpunktfarbig (22). Das längste bekannte Fantasie- Isogramm (mit Sonderbuchstaben) ist Heizölrückstoßabdämpfung mit 24 Buchstaben.
Ein Isogramm würde sich also auch gut als Schlüsselwort eignen!

Ein ***Pangramm*** *ist ein Satz, der alle Buchstaben des Alphabets enthält. Ein echtes Pangramm muss auch gleichzeitig ein Isogramm sein, d.h. alle Buchstaben des Alphabets genau einmal enthalten. Echte Pangramme mit den lateinischen Buchstaben sind sehr schwierig zu finden, mit nur natürlichen Wörtern ist in keiner Sprache mit lateinischer Schrift eines bekannt.*

„Das wohl erste echte deutschsprachige Pangramm mit Sonderbuchstaben wurde im Jahr 2003 in einer Newsgroup veröffentlicht: „Fix, Schwyz!“ quäkt Jürgen blöd vom Paß. Dieser Satz folgt allerdings nur der deutschen Orthographie vor der Rechtschreibreform von 1996.“
Aus http://de.wikipedia.org/wiki/Pangramm

Weitere deutsche Pangramme sind:
Vogel Quax zwickt Johnys Pferd Bim. (29 Buchstaben)
Sylvia wagt quick den Jux bei Pforzheim. (33 Buchstaben)
oder mit Umlauten und ß:
Zwölf Boxkämpfer jagen Viktor quer über den großen Sylter Deich. (54 Buchstaben)

Solche Pangramme kann man auch verwenden, um ganze Geheimtextalphabete zu erzeugen: dabei lässt man einfach die Buchstaben, die schon einmal vorgekommen sind, weg. Der Vorteil ist, dass man sich einen lustigen Satz ja leicht merken kann.

Im Japanischen ist sogar ein echtes Pangramm bekannt: die Iroha, ein Gedicht, das alle 50 ursprüngliche Silben der japanischen Schrift enthält, und das ohne Wiederholungen!

Zusammenfassung monoalphabetische Substitutionschiffren:

Die Buchstaben des Klartextes behalten ihre Position. Die Buchstaben des Klartextalphabets werden durch einen Buchstaben oder ein Zeichen eines bestimmten Geheimtextalphabets ersetzt. (Es gibt genau ein Geheimtextalphabet.)

Additive Chiffre, Verschiebechiffre („Cäsar- Verschlüsselung“)

Schlüssel: Eine Zahl t zwischen 0 und 25

Chiffrieren: Wenn x die Nummer des Klartextbuchstabens ist, dann ist (x+t)mod26 die Nummer des Geheimtextbuchstaben.

Dechiffrieren: Wenn y die Nummer des Geheimtextbuchstabens ist, dann ist (y-t)mod26 die Nummer des Klartextbuchstabens.

Multiplikative Chiffre

Schlüssel: Eine Zahl s aus {1,3,5,7,9,11,15,17,19,21,23,25}

Chiffrieren: Wenn x die Nummer des Klartextbuchstabens ist, dann ist (s.x)mod26 die Nummer des Geheimtextbuchstaben.

Dechiffrieren: Wenn y die Nummer des Geheimtextbuchstabens ist, dann ist (y.s’)mod26 die Nummer des Klartextbuchstabens. Dabei ist s.s’mod26 = 1.

Tauschchiffre, affine Chiffre

Schlüssel: Ein Zahlenpaar (s,t) mit s aus {1,3,5,7,9,11,15,17,19,21,23,25} und t zwischen 0 und 25

Chiffrieren: Wenn x die Nummer des Klartextbuchstabens ist, dann ist (s.x+t)mod26 die Nummer des Geheimtextbuchstaben.

Dechiffrieren: Wenn y die Nummer des Geheimtextbuchstabens ist, dann ist (y-t).s'mod26 die Nummer des Klartextbuchstabens. Dabei ist s.s'mod26 = 1.

Schlüsselwortchiffre

Schlüssel: Ein Wort: dieses Wort bildet ohne Wiederholung schon vorgekommener Buchstaben den Anfang des Geheimtextalphabets, welches durch die restlichen Buchstaben in alphabetischer Reihenfolge aufgefüllt wird. (Dabei kann nach dem Schlüsselwort entweder mit A begonnen werden, oder mit dem auf den letzten Schlüsselwortbuchstaben folgenden Buchstaben des Alphabets.)

Chiffrieren: Jeder Buchstabe des Klartextalphabets wird durch den entsprechenden Buchstaben des Geheimtextalphabets ersetzt.

Dechiffrieren: Jeder Buchstabe des Geheimtextalphabets wird durch den entsprechenden Buchstaben des Klartextalphabets ersetzt.

Schlüsselwortchiffre mit Schlüsselbuchstaben

Schlüssel: Ein Wort und ein Schlüsselbuchstabe: dieses Wort ohne Wiederholung schon vorgekommener Buchstaben wird, beginnend beim Schlüsselbuchstaben, unter das Klartextalphabet geschrieben. Nach dem Schlüsselwort wird das Geheimtextalphabet durch die restlichen Buchstaben in alphabetischer Reihenfolge aufgefüllt.

Chiffrieren: Jeder Buchstabe des Klartextalphabets wird durch den entsprechenden (darunter stehenden) Buchstaben des Geheimtextalphabets ersetzt.

Dechiffrieren: Jeder Buchstabe des Geheimtextalphabets wird durch den entsprechenden (darüber stehenden) Buchstaben des Klartextalphabets ersetzt.

2.2. Kryptoanalyse von monoalphabetischen Chiffren

Beim Versuch, einen Geheimtext zu entschlüsseln, gibt es verschiedene Herangehensweisen. Man geht grundsätzlich davon aus, dass der Kryptoanalytiker den verwendeten Chiffrieralgorithmus kennt oder erraten kann, da dieser meist schwer geheim zu halten ist. Um den Geheimtext zu entschlüsseln muss er also herausfinden, welcher Schlüssel verwendet wurde. Daraus folgt:

Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels. (Prinzip von Kerckhoffs)

2.2.1. Systematische Schlüsselsuche

Eine Methode, eine Chiffre zu brechen ist die **Systematische Schlüsselsuche**, auch Exhaustionsmethode oder Brute-Force-Methode (englisch für Methode der rohen Gewalt) genannt. Dabei werden systematisch alle möglichen Schlüssel durchprobiert. Dabei braucht man höchstens so viele Versuche, wie es Schlüssel gibt.
Verschiebechiffren und Multiplikative Chiffren können damit leicht geknackt werden, da die Anzahl der Schlüssel relativ klein ist. Bei Schlüsselwortchiffren ist die Anzahl der möglichen Schlüssel schon sehr viel größer, hier wäre ein Mensch mit der Schlüsselsuche ziemlich chancenlos.
Allerdings kann man viele einfache monoalphabetische Chiffren knacken, indem man die systematische Schlüsselsuche von einem Computer durchführen lässt.

2.2.2. Mustersuche

Eine weitere Möglichkeit ist die sogenannte **Mustersuche** (oder auch „Methode des wahrscheinlichen Wortes“). Wenn man weiß, errät oder auch nur vermutet, dass in einem Geheimtext ein bestimmtes Wort oder eine bestimmte Phrase, genannt **Crib**, auftritt, dann kann man diese Methode verwenden. Gelingt es nämlich, die genaue Lage des Cribs zu bestimmen, dann reicht das bei der monoalphabetischen Verschlüsselung meist schon aus, um den Geheimtext zu knacken.

Ein Beispiel:
Es liegt folgender Geheimtext vor, bei dem man vermutet, dass er monoalphabetisch verschlüsselt wurde:

```
FVMZM FGMJZ QDGKK RGCRI KJZMR GQQQP LWWZI
JZDVZ AZWQJ GIKZQ DZIMP IZEZM FZVKJ
```

Man vermutet oder weiß, dass die Nachricht für oder von „Max Mustermann“ ist oder von ihm handelt. Deshalb nimmt man an, dass dieser Name im Geheimtext verschlüsselt auftaucht. Um die genaue Lage des wahrscheinlichen Worts herauszufinden, geht man wie folgt vor:

Man bestimmt das Muster des Cribs und nummeriert die Buchstaben durch, wobei gleiche Buchstaben gleiche Nummern erhalten.

Wahrscheinliches Wort: M A X M U S T E R M A N N

Muster: **1 2 3 1 4 5 6 7 8 1 2 9 9**

Danach überprüft man für jede mögliche Lage des Cribs im Geheimtext das Muster dieses Geheimtextfragments. Der Geheimtext ist 65 Buchstaben und das wahrscheinliche Wort 13 Buchstaben lang. Also sind 65-12=53 Lagen möglich. (Weil das wahrscheinliche Wort kann beim ersten, zweiten, dritten,…bis zum 53.Buchstaben des Geheimtextes beginnen, würde es bei einem der letzten 12 Buchstaben beginnen, gehen sich die 13 Buchstaben des Wortes nicht mehr aus.)

Lage 1: F V M Z M F G M J Z Q D G

Muster 1: 1 2 3 4 3 1 5 3 6 4 7 8 9

Lage 2: V M Z M F G M J Z Q D G K

Muster 2: 1 2 3 2 4 5 2 6 3 7 8 5 9

...

Lage 16: R G C R I K J Z M R G Q Q

Muster 16: **1 2 3 1 4 5 6 7 8 1 2 9 9**

...

Lage 53: I M P I Z E Z M F Z V K J

Muster 53: 1 2 3 1 4 5 4 2 6 4 7 8 9

Nur bei Lage 16 stimmt das Muster des Geheimtextes mit dem Muster des wahrscheinlichen Wortes überein. Also kann das Wort, falls es wirklich im Geheimtext vorkommt, nur an dieser Stelle stehen.

Man schreibt nun das Wort über die vermutliche Lage im Geheimtext

```
..... ..... ..... maxmu sterm ann.. .....
FVMZM FGMJZ QDGKK RGCRI KJZMR GQQQP LWWZI
..... ..... ..... ..... ..... .....
JZDVZ AZWQJ GIKZQ DZIMP IZEZM FZVKJ
```

und ergänzt auch die restlichen somit identifizierten Buchstaben (R=m, G=a, C=x, I=u, K=s, J=t, Z=e, M=r, G=a und Q=n)

```
..rer .arte n.ass maxmu sterm annn. ...eu
FVMZM FGMJZ QDGKK RGCRI KJZMR GQQQP LWWZI
te..e .e.nt ausen .eur. ue.er .e.st
JZDVZ AZWQJ GIKZQ DZIMP IZEZM FZVKJ
```

Die weitere Entzifferung ist in diesem Fall nicht mehr schwierig, da nun einige leicht zu erratende Klartextfragmente vorhanden sind, z.B. er.arten = erwarten, .ass = dass, .eute = heute, .e.ntausen. = zehntausend, usw.
Der Klartext lautet also:

```
Wir erwarten dass Max Mustermann noch heute die zehntausend Euro überweist.
```

Da bei Schlüsselwortchiffren oder bei Chiffren mit willkürlich permutierten Geheimtextalphabeten die Anzahl der möglichen Schlüssel zu groß ist und man auch selten einen Crib hat, um die Mustersuche anzuwenden, braucht man eine andere Methode um diese Chiffren zu knacken.
Lange Zeit erkannte niemand die Schwachstelle der monoalphabetischen Substitution, doch dann entdeckte man, dass man die monoalphabetische Substitution relativ leicht brechen kann, indem man ein statistisches Verfahren verwendet…

2.2.3. Die Geschichte der Kryptoanalyse

Der Ursprung der Kryptoanalyse liegt im Orient. Die Araber verwendeten Mitte des ersten Jahrtausends monoalphabetische Verschlüsselungsverfahren. Sie waren aber nicht nur in der Lange diese Verfahren anzuwenden, den arabischen Kryptoanalytikern gelang es schließlich auch als erster, diese Verfahren zu brechen.

Von großer Bedeutung für die Erfindung der Kryptoanalyse waren theologische Studien. Die Theologen wollten die zeitliche Reihenfolge der Offenbarungen Mohammeds erkunden und zählten deshalb die Häufigkeit der einzelnen Wörter in jeder Offenbarung, da man annahm, dass manche Wörter erst später entstanden waren. Sie untersuchten auch weitere Texte, die Hadīth (Überlieferungen über Äußerungen Mohammeds), um festzustellen, ob die Aussagen wirklich von

Mohammed selbst stammten. Dazu wurden Herkunft der Wörter und Satzbau studiert.
Wichtig für die Kryptoanalyse ist aber, dass die Theologen nicht nur auf der Ebene der Wörter blieben, sondern auch einzelne Buchstaben überprüften. Dabei stellte man insbesondere fest, dass manche Buchstaben häufiger vorkommen als andere. Im Arabischen kommen die Buchstaben „a“ und „l“ am häufigsten vor, zum Teil wegen des Artikels „al“. Diese Beobachtungen legten den Grundstein für die Kryptoanalyse.

Der arabische Gelehrte Al-Kindi (voller Name Abu Yusuf Yaqub ibn Is-haq ibn as Sabbah ibn 'omran ibn Ismail Al-Kindi) schrieb ca.750 n.Chr. das erste uns bekannte Buch über Kryptoanalyse mit dem Titel „Schrift über das Entziffern kryptographischer Botschaften“. Seine revolutionäre Methode der Kryptoanalyse, die sogenannte ***Häufigkeitsanalyse****, beruht auf der Tatsache, dass jeder Buchstabe in einer gewissen Sprache durchschnittlich mit einer ganz bestimmten Häufigkeit vorkommt.*

In Al-Kindis Werk ist seine Entschlüsselungsmethode in zwei Abschnitten beschrieben:
„Eine Möglichkeit, eine verschlüsselte Botschaft zu entziffern, vorausgesetzt, wir kennen ihre Sprache, besteht darin, einen anderen Klartext in der selben Sprache zu finden, der lang genug ist, um ein oder zwei Blätter zu füllen, und dann zu zählen, wie oft jeder Buchstabe vorkommt. Wir nennen den häufigsten Buchstaben den ‚ersten’, den zweithäufigsten den ‚zweiten’, den folgenden den ‚dritten’ und so weiter, bis wir alle Buchstaben in der Klartextprobe durchgezählt haben.
Dann betrachten wir den Geheimtext, den wir entschlüsseln wollen, und ordnen auch seine Symbole. Wir finden das häufigste Symbol und geben ihm die Gestalt des ‚ersten’ Buchstabens der Klartextprobe, das zweithäufigste Symbol wird zum ‚zweiten’ Buchstaben, das dritthäufigste zum ‚dritten’ Buchstaben und so weiter, bis wir alle Symbole des Kryptogramms, das wir entschlüsseln wollen, auf diese Weise zugeordnet haben.“
Aus Simon Singh: Codes, Seite 34,35

2.2.4. Häufigkeitsanalyse

In jeder Sprache kommen die Buchstaben mit einer ganz bestimmten Häufigkeit vor. Diese Häufigkeiten kann man ermitteln, indem man sehr lange Texte betrachtet und die relativen Buchstabenhäufigkeiten ermittelt.
Im Deutschen kommt zum Beispiel der Buchstabe „e“ mit Abstand am häufigsten vor (17,40%). Die häufigsten 10 Buchstaben (e,n,i,s,r,a,t,d,h,u) machen schon über drei Viertel eines Textes aus!

Eine Tabelle der Buchstabenhäufigkeiten der deutschen Sprache:
(Die Umlaute ä, ö und ü wurden wie ae, oe und ue gezählt)

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 %

Platz	Buchstabe	Relative Häufigkeit
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.	J	0,27 %
24.	Y	0,04 %
25.	X	0,03 %
26.	Q	0,02 %

Aus Albrecht Beutelspacher: Kryptologie, 7.Auflage, Seite 10

Wird nun ein deutscher Text mittels monoalphabetischer Substitution chiffriert, bleiben die Buchstabenhäufigkeiten erhalten, nur sind die einzelnen Häufigkeiten dann anderen Buchstaben zugeordnet. Wenn der Buchstabe „e“ durch ein X ersetzt wird, dann ist mit großer Wahrscheinlichkeit X der häufigste Geheimtextbuchstabe (wenn der Text lang genug ist).
Kurze Texte weichen häufig von dieser Verteilung ab, deshalb ist die Entschlüsselung mittels Häufigkeitsanalyse bei Texten unter hundert Buchstaben sehr schwierig. Natürlich kann es auch bei langen Texten zu Abweichungen der

Buchstabenhäufigkeiten kommen, zum Beispiel kommt in dieser Arbeit sehr oft das Wort „Text“ vor, also wird das „x“ viel häufiger vorkommen, als die durchschnittlichen 0,03%. Deshalb muss man bei der Kryptoanalyse eines Geheimtextes auch etwas vorsichtiger vorgehen, als bei Al-Kindis Anleitung.

Für viele Schriftsteller war es eine Herausforderung, bestimmte Buchstaben nicht zu verwenden. Am berühmtesten ist wohl der Roman „La Disparation“ des französischen Schriftstellers Georges Perec, der in diesem 200 Seiten langen Roman kein einziges Mal den Buchstaben „e“ verwendete.
Eugen Helmlé schaffte es sogar, den Roman ins Deutsche zu übersetzten und dabei, wie in der Originalfassung, kein „e“ zu verwenden. Seine Übersetzung trägt den Titel „Anton Voyls Fortgang“.

Ein Beispiel: (aus Simon Singh: Codes, Seite 38ff)
Die Entschlüsselung eines Geheimtextes:
PR ISRSQ YSPUD SYOCREBS GPS NFRZB GSY NCYBVEYCWDPS SPRS ZVOUDS HVOONVQQSRDSPB, GCZZ GPS NCYBS SPRSY SPRMPESR WYVHPRM GSR YCFQ SPRSY ECRMSR ZBCGB SPRRCDQ FRG GPS NCYBS GSZ YSPUDZ GSR SPRSY WYVHPRM. QPB GSY MSPB ASTYPSGPEBSR GPSZS FSASYQCSZZPE EYVZZSR NCYBSR PRUDB OCSRESY, FRG QCR SYZBSOOBS SPRS NCYBS GSZ YSPUDZ, GPS ESRCF GPS EYVSZZS GSZ YSPUDZ DCBBS.
AVYESZ, HVR GSY ZBYSRES GSY JPZZSRZUDCTB

Wenn man weiß (oder auch nur vermutet), dass dieser Text mittels monoalphabetischer Substitution verschlüsselt wurde, ist es praktisch unmöglich, alle möglichen Schlüssel durchzuprobieren. Deshalb versuchen wir, den Geheimtext mittels Häufigkeitsanalyse zu dechiffrieren.
Dazu erstellt man eine Häufigkeitstabelle:

Buchstabe	Absolute Häufigkeit	Relative Häufigkeit
S	67	20,49 %
R	32	9,79 %
P	30	9,17 %
Y	29	8,87 %
Z	24	7,34 %
B	20	6,12 %
G	20	6,12 %
C	18	5,50 %
E	12	3,67 %
D	11	3,36 %
V	10	3,06 %
Q	8	2,45 %
O	7	2,14 %

Buchstabe	Absolute Häufigkeit	Relative Häufigkeit
U	7	2,14 %
N	7	2,14 %
F	6	1,83 %
M	5	1,53 %
H	4	1,22 %
W	3	0,92 %
A	3	0,92 %
T	2	0,61 %
I	1	0,31 %
J	1	0,31 %
K	0	0,0 %
L	0	0,0 %
Y	0	0,0 %

Zuerst betrachten wir die fünf häufigsten Buchstaben, S, R, G, C, E. Da S mit Abstand am häufigsten vorkommt, gehen wir davon aus, dass es für den häufigsten Buchstaben in der deutschen Sprache, nämlich e, steht. Also nehmen wir an, dass **S = e**. Die nächsten vier Buchstaben R, G, C, E stehen wahrscheinlich für die zweit- bis fünfthäufigsten Buchstaben im Deutschen n, i, s, und r, jedoch wissen wir noch nicht, in welcher Reihenfolge.

Dazu müssen wir die Häufigkeitsanalyse verfeinern und betrachten die im Deutschen häufigsten Bigramme (Paare aufeinanderfolgender Buchstaben).

Bigramm	Relative Häufigkeit
en	3,88%
er	3,75%
ch	2,75%
te	2,26%
de	2,00%
nd	1,99%
ei	1,88%
ie	1,79%
in	1,67%
es	1,52%

Aus Albrecht Beutelspacher: Kryptologie, 7.Auflage, Seite 17

Wir zählen, wie oft Bigramme von S, unserem mutmaßlichen „e“, und einem der zweit- bis fünfhäufigsten Buchstaben R, G, C, E vorkommen.
Diese müssten für en/ne, ei/ie, es/se und er/re stehen.

Bigramm	Absolute Häufigkeit
SR/RS	13/7
SP/PS	13/8
SY/YS	11/5
SZ/ZS	7/4

Wir nehmen an, dass die drei häufigsten Bigramme SR, SP und SY den häufigsten Bigrammen mit e im Deutschen, en, er und ei entsprechen. Daher müsste es sich bei SZ und ZS um es und se handeln.
Um herauszufinden, welche Geheimtextbuchstaben für n und i stehen, betrachten wir das im Deutschen häufigste Trigramm: „ein“. Es kommen nur SPR, SRP, SPY, SYP, SRY und SYR in Frage. Da davon nur SPR als Wort im Text vorkommt (und zwar siebenmal), schließen wir daraus **P=i** und **R=n**.
Um sicherzustellen, dass unsere Vermutung Z=s, und daher auch Y=r, stimmt (und nicht umgekehrt) machen wir zuerst das d ausfindig und nutzen dann den Umstand, dass „der“ öfter vorkommt als „des“.
Das häufigste Wort im Deutschen ist „die“. Da wir schon wissen dass PS für ie steht, sehen wir gleich, dass GPS fünfmal im Geheimtext vorkommt und vermuten dass **G=d**.
Wir überprüfen die Häufigkeiten von GSY und GSZ, die „der“ und „des“ entsprechen müssten. GSY kommt viermal vor, GSZ aber auch dreimal. Zusammen mit der Tatsache, dass das Bigramm SY auch öfters vorkommt, als SZ, können wir uns ziemlich sicher sein, dass **Y=r** und **Z=s**.
Damit haben wir die fünf häufigsten Buchstaben mit einiger Sicherheit entschlüsselt und können diese Klartextbuchstaben in den Geheimtext einsetzen:

in IeneQ reiUD erOCnEBe die NFnsB der NCrBVErCWDie eine sVOUDe HVOONVQQenDeiB, dCss die NCrBe einer einMiEen WrVHinM den rCFQ einer ECnMen sBCdB einnCDQ Fnd die NCrBe des reiUDs den einer WrVHinM. QiB der MeiB AeTriediEBen diese FeAerQCessiE ErVssen NCrBen niUDB OCenEer, Fnd

QCn ersBeOOBe eine NCrBe des reiUDs, die EenCF die ErVesse des reiUDs DCBBe.
AVrEes, HVn der sBrenEe der JissensUDCTB

Nachdem wir nun einen Teil des Klartextes kennen können wir vielleicht einige Buchstaben erraten.
„dCss“ könnte zum Beispiel „dass“ heißen und unsere Vermutung wird bestätigt, weil das C ein relativ häufiger Geheimtextbuchstabe ist (Platz 8 der Häufigkeitstabelle und „a“ ist im Deutschen der sechsthäufigste Buchstabe).
Hinter „reiUD“ könnte das Wort „reich“ stecken (da die Buchstaben s, e und n schon vergeben sind), c und h sind außerdem relativ seltene Buchstaben, aber sie bilden ein sehr häufiges Paar. Im Geheimtext kommt UD ganze siebenmal vor und das bestätigt auch diese Annahme.
Bei „Fnd“ könnte man noch das Wort „und“ vermuten.

Nun setzen wir auch die geratenen Klartextbuchstaben **C=a**, **U=c**, **D=h** und **F=u** in den Geheimtext ein und hoffen, dass sich etwas Sinnvolles ergibt:

in IeneQ reich erOanEBe die NFnsB der NarBVEraWhie eine sVOche HVOONVQQenheiB, dass die NarBe einer einMiEen WrVHinM den rauQ einer EanMen sBadB einnahQ und die NarBe des reichs den einer WrVHinM. QiB der MeiB AeTriediEBen diese ueAerQaessiE ErVssen NarBen nichB OaenEer, und Qan ersBeOOBe eine NarBe des reichs, die Eenau die ErVesse des reichs DaBBe.
AVrEes, HVn der sBrenEe der JissenschaTB

Einen weiteren sehr häufigen Geheimtextbuchstaben, das B (Platz 6), finden wir in „sBadB“ und in „nichB“. Da liegt die Vermutung nahe, dass es sich um das „t“ (siebenthäufigster Buchstabe im Deutschen) handelt, also **B=t**.
Wir setzen noch einmal ein:

in IeneQ reich erOanEte die NFnst der NartVEraWhie eine sVOche HVOONVQQenheit, dass die Narte einer einMiEen WrVHinM den rauQ einer EanMen stadt einnahQ und die Narte des reichs den einer WrVHinM. Qit der Meit

AeTriediEten diese ueAerQaessiE ErVssen Narten nicht OaenEer, und Qan ersteOOte eine Narte des reichs, die Eenau die ErVesse des reichs Datte.
AVrEes, HVn der strenEe der JissenschaTt

Wir sehen, dass „Eenau“ nur „genau“ heißen kann, dass das letzte Wort „wissenschaft“ heißen muss und dass „einnahQ“ wahrscheinlich einnahm heißt. (**E=g**, **J=w, T=f** und **Q=m**)

in Ienem reich erOangte die NFnst der NartVgraWhie eine sVOche HVOONVmmenheit, dass die Narte einer einMigen WrVHinM den raum einer ganMen stadt einnahm und die Narte des reichs den einer WrVHinM. mit der Meit Aefriedigten diese ueAermaessig grVssen Narten nicht Oaenger, und man ersteOOte eine Narte des reichs, die genau die grVesse des reichs Datte.
AVrges, HVn der strenge der wissenschaft

Nun könnte man so weiterraten, doch vielleicht können wir aus den bekannten Buchstaben den verwendeten Schlüssel schon erkennen:

Klartext:	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
Geheimtext:	C	–	U	G	S	T	E	D	P	-	-	-	Q	R	-	-	-	Y	Z	B	-	-	J	-	-	-

Man sieht, dass diese Chiffre ziemlich sicher mittels Schlüsselwort erzeugt worden ist. (Q und R hintereinander, Y, Z, B hintereinander im Geheimtextalphabet)

Hier könnte man schon erraten, dass das Schlüsselwort der Name einer Romanfigur aus einer Erzählung von Edgar Allen Poe ist: „C. Auguste Dupin“.
Ansonsten müsste man noch einige Buchstaben herausfinden, um das Geheimtextalphabet weiter aufzufüllen und den Schlüssel zu erraten: z.B. „grVssen“ heißt wahrscheinlich „grossen“, „erOangte“ steht für „erlangte“ und „ganMen“ wird „ganzen“ heißen.

Schlussendlich bekommt man das vollständige Geheimtextalphabet:

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

und den vollständigen Klartext:

In jenem Reich erlangte die Kunst der Kartographie eine solche Vollkommenheit, dass die Karte einer einzigen Provinz den Raum einer ganzen Stadt einnahm und die Karte des Reichs den einer Provinz. Mit der Zeit befriedigten diese uebermaessig grossen Karten nicht laenger, und man erstellte eine Karte des Reichs, die genau die Groesse des Reichs hatte.
Borges, von der Strenge der Wissenschaft

Jede monoalphabetische Chiffrierung einer natürlichen Sprache kann also relativ leicht mittels Häufigkeitsanalyse geknackt werden!

Aufgaben:

1. Wie würdest du vorgehen, wenn du eine einfache Verschiebechiffre („Cäsar-Verschlüsselung“) mittels Häufigkeitsanalyse brechen willst?

Lösung:
Nachdem man die einzelnen Buchstabenhäufigkeiten im Geheimtext festgestellt hat, nimmt man an, dass der häufigste Buchstabe dem „e“ entspricht. Dadurch weiß man auch, um wie viele Stellen das Geheimtextalphabet verschoben ist. Mit diesem Geheimtextalphabet entschlüsselt man den Geheimtext.
(Sollte dabei kein sinnvoller Text herauskommen, nimmt man an, dass der zweithäufigste Buchstabe das „e“ ist.)

2. Versuche, folgenden Geheimtext mittels Häufigkeitsanalyse zu entschlüsseln! (Hinweis: es wurde eine Verschiebechiffre benutzt)
XCY GUNBYGUNCE CMN XCY QCMMYHMWBUZN, QYFWBY UOM XYL OHNYLMOWBOHA PIH ZCAOLYH OHX XYG LYWBHYH GCN TUBFYH YHNMNUHX. ZOYL GUNBYGUNCE ACVN YM EYCHY UFFAYGYCH UHYLEUHHNY XYZCHCNCIH, BYONY QCLX MCY OYVFCWBYLQYCMY UFM YCHY QCMMYHMWBUZN, XCY MYFVMN AYMWBUZZYHY UVMNLUENY MNLOENOLYH UOZ CBLY YCAYHMWBUZNYH OHX GOMNYL OHNYLMOWBN, VYMWBLCYVYH.

Lösung:

Die Häufigkeitsanalyse ergibt:

Y	H	N	C	M	U	O	B	L	W	X	Z	G	F	E	A	V	Q	I	P	T	J	K	R	S	D
50	27	24	24	23	18	16	15	15	10	10	9	8	7	6	6	6	5	2	1	1	0	0	0	0	0

Der Buchstabe Y kommt mit fast 18% am häufigsten vor, d.h. das Y entspricht wahrscheinlich dem „e“. Das Klartextalphabet wurde also um 20 Stellen verschoben:

Klartextalphabet: 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
Geheimtextalphabet: 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

Der Klartext lautet:

Die Mathematik ist die Wissenschaft, welche aus der Untersuchung von Figuren und dem Rechnen mit Zahlen entstand. Für Mathematik gibt es keine allgemein anerkannte Definition; heute wird sie üblicherweise als eine Wissenschaft, die selbst geschaffene abstrakte Strukturen auf ihre Eigenschaften und Muster untersucht, beschrieben.

Aus http://de.wikipedia.org/wiki/Mathematik

3. Erstelle eine Häufigkeitstabelle des folgenden Geheimtextes! Zähle alle Bigramme der zweit- bis siebenthäufigsten Buchstaben mit dem mutmaßlichen „e“! Kannst du damit die Buchstaben „d, i, n, r, s“ zu erkennen? Setze die Buchstaben in den Geheimtext ein und versuche, das restliche Geheimtextalphabet zu erraten! (Hinweis: Schlüsselwortchiffre)

XUJY SUN UOSU SUX OUZOGUIOYUO KVIWIZOSUWYX, AUWUJOGUMY XRIPO XUJY SUW VOYJLU, BJWS SJU NVYIUNVYJL JO CPWN APO YIUPWJUO QWVUXUOYJUWY, SJU NJY VZXXVHUO EUHJOOUO, BUMRIU VMX BVIW VOHUXUIUO BUWSUO, SVWVZX BUWSUO SVOO BUJYUWU BVIWU VZXXVHUO IUWHUMUJYUY. SJUXU IUWMUJYZOH HUXRIJUIY SVEUJ OVRI HUOVZ CUXYHUMUHYUO XRIMZXXWUHUMO. SJU VZXXVHUO, NJY SUOUO SJU YIUPWJU VOCVUOHY, OUOOY NVO VDJPNU, SJU SVWVZX IUWHUMUJYUYUO OUOOY NVO XVUYGU. SJU IUWMUJYZOH XUMEXY JXY UJO EUBUJX SUX XVYGUX. JO SUW QWVDJX XQJUMUO OPRI SUCJOJYJPOUO UJOU WPMMU, XJU HUIPUWUO VEUW GZN IVOSBUWLXGUZH SUW MPHJL, SVX APWVZXHUXUYGY BJWS. VZCHWZOS

SJUXUX VZCEVZX SUW NVYIUNVYJXRIUO YIUPWJUO EUGUJRIOUY NVO XJU VMX VDJPNVYJXRIU YIUPWJUO.

Lösung:

Die Häufigkeitsanalyse ergibt:

Buchstabe	Absolute Häufigkeit	Relative Häufigkeit
U	118	20,17 %
O	60	10,26%
J	49	8,38%
V	44	7,52%
X	44	7,52%
Y	40	6,84%
W	35	5,98%
S	30	5,13%
I	28	4,79%
H	20	3,42%
Z	18	3,08%
M	16	2,74%
P	15	2,56%

Buchstabe	Absolute Häufigkeit	Relative Häufigkeit
N	14	2,39%
B	10	1,71%
G	9	1,54%
R	8	1,37%
E	7	1,20%
C	6	1,03%
L	4	0,68%
D	3	0,51%
A	3	0,51%
Q	3	0,51%
K	1	0,17%
T	0	0,00%
F	0	0,00%

Der mit Abstand häufigste Buchstabe entspricht ziemlich sicher dem „e“, also **e=U**. Zählt man alle möglichen Bigramme der nächsten 6 Buchstaben O, J, V, X, Y, W mit dem mutmaßlichen „e“, erhält man folgende Tabelle:

Bigramm	Absolute Häufigkeit
UO/OU	23/4
UJ/JU	13/17
UV/VU	0/3
UX/XU	11/8
UY/YU	5/2
UW/WU	17/5

Die vier häufigsten mit U beginnenden Bigramme UO, UJ, UX und UW stehen wahrscheinlich für die häufigsten Bigramme mit „e“ im Deutschen: „en“, „er“ und „ei“ und „es“.

Wir betrachten nun das häufigste Trigramm im eutschen: „ein“. Es kommen nur UOJ, UOX, UOW, UJO, UJX, UJW, UXO, UXJ, UXW, UWO, UWJ und UWX in Frage: UJO

kommt im Text 3 Mal und UJX 1 Mal vor. Wir nehmen deshalb an, dass UJO für „ein“ steht und vermuten: **J=i** und **O=n**.
Um nun auch noch „r“ und „s“ zu unterscheiden (es kommen noch X und W in Frage), betrachten wir zuerst das häufigste Wort im Deutschen: „die“. Wir wissen schon, dass JU für „ie“ steht. Im Text kommt SJU als Wort 6 Mal vor, also **S=d**. Um „r“ und „s“ zu bestimmen, nutzen wir die Tatsache, dass „der“ durchschnittlich öfter vorkommt als „des“. SUX kommt nur 2 Mal vor, während SUW 4 Mal vorkommt. Also **X=s** und **W=r**.

Nun setzen wir die geratenen Klartextbuchstaben in den Geheimtext ein:
seiY deN ende des neZnGeInYen KVIrIZnderYs, AereinGeMY sRIPn seiY der VnYiLe, Bird die NVYIeNVYiL in CPrN APn YIePrien QrVesenYierY, die NiY VZssVHen EeHinnen, BeMRIe VMs BVIr VnHeseIen Berden, dVrVZs Berden dVnn BeiYere BVIre VZssVHen IerHeMeiYeY. diese IerMeiYZnH HesRIieIY dVEei nVRI HenVZ CesYHeMeHYen sRIMZssreHeMn. die VZssVHen, NiY denen die YIePrie VnCVenHY, nennY NVn VDiPNe, die dVrVZs IerHeMeiYeYen nennY NVn sVeYGe. die IerMeiYZnH seMEsY isY ein EeBeis des sVYGes. in der QrVDis sQieMen nPRI deCiniYiPnen eine rPMMe, sie HeIPeren VEer GZN IVndBerLsGeZH der MPHiL, dVs APrVZsHeseYGY Bird. VZCHrZnd dieses VZCEVZs der NVYIeNVYisRIen YIePrien EeGeiRIneY NVn sie VMs VDiPNVYisRIe YIePrien.

Die Wörter „seiY“, „nennY“ und „isY“ legen nahe, dass **Y=t**. Das Wort „Bird“ kann auch nur „wird“ bedeuten, d.h. **B=w**.
Wir erhalten:

seit deN ende des neZnGeInten KVIrIZnderts, AereinGeMt sRIPn seit der VntiLe, wird die NVtIeNVtiL in CPrN APn tIePrien QrVesentiert, die Nit VZssVHen EeHinnen, weMRIe VMs wVIr VnHeseIen werden, dVrVZs werden dVnn weitere wVIre VZssVHen IerHeMeitet. diese IerMeitZnH HesRIieIt dVEei nVRI HenVZ CestHeMeHten sRIMZssreHeMn. die VZssVHen, Nit denen die tIePrie VnCVenHt, nennt NVn VDiPNe, die dVrVZs IerHeMeiteten nennt NVn sVetGe. die IerMeitZnH seMEst ist ein Eeweis des sVtGes. in der QrVDis sQieMen nPRI deCinitiPnen eine rPMMe, sie HeIPeren VEer GZN IVndwerLsGeZH der MPHiL, dVs APrVZsHesetGt

wird. VZCHrZnd dieses VZCEVZs der NVtIeNVtisRIen tIePrien EeGeiRInet NVn sie VMs VDiPNVtisRIe tIePrien.

Wir vermuten, dass „Nit“ „mit“ bedeutet (**N=m**) und da das „e“ schon vergeben ist, kann „dVnn“ nur „dann“ heißen (**V=a**). Also:

seit dem ende des neZnGeInten KaIrIZnderts, AereinGeMt sRIPn seit der antiLe, wird die matIematiL in CPrm APn tIePrien Qraesentiert, die mit aZssaHen EeHinnen, weMRIe aMs waIr anHeseIen werden, daraZs werden dann weitere waIre aZssaHen IerHeMeitet. diese IerMeitZnH HesRIieIt daEei naRI HenaZ CestHeMeHten sRIMZssreHeMn. die aZssaHen, mit denen die tIePrie anCaenHt, nennt man aDiPme, die daraZs IerHeMeiteten nennt man saetGe. die IerMeitZnH seMEst ist ein Eeweis des satGes. in der QraDis sQieMen nPRI deCinitiPnen eine rPMMe, sie HeIPeren aEer GZm IandwerLsGeZH der MPHiL, das APraZsHesetGt wird. aZCHrZnd dieses aZCEaZs der matIematisRIen tIePrien EeGeiRInet man sie aMs aDiPmatisRIe tIePrien.

Bei „matIematiL“ erkennen wir natürlich sorfort das Wort „mathematik“, „antiLe“ heißt ziemlich sicher „antike“ und „daraZs“ muss „daraus“ heißen. Also **I=h**, **L=k** und **Z=u** und somit:

seit dem ende des neunGehnten Kahrhunderts, AereinGeMt sRhPn seit der antike, wird die mathematik in CPrm APn thePrien Qraesentiert, die mit aussaHen EeHinnen, weMRhe aMs wahr anHeseIen werden, daraus werden dann weitere wahre aussaHen IerHeMeitet. diese herMeitnH HesRhieht daEei naRh Henau CestHeMeHten sRhMussreHeMn. die aussaHen, mit denen die thePrie anCaenHt, nennt man aDiPme, die daraus herHeMeiteten nennt man saetGe. die herMeitunH seMEst ist ein Eeweis des satGes. in der QraDis sQieMen nPRI deCinitiPnen eine rPMMe, sie HehPeren aEer Gum handwerksGeuH der MPHik, das APrausHesetGt wird. auCHrund dieses auCEaus der mathematisRhen tiePrien EeGeiRinet man sie aMs aDiPmatisRhe thePrien.

Jetzt kann man leicht erraten: „neunGehnten“, „Qraesentiert“, „Henau“, „saetGe“, „Eweis“, „mathematisRhen“, usw.

Also G=z, Q=p, H=g, G=z, E=b, R=c: Wir könnten nun wieder einsetzen und weiterraten, oder wir betrachten einmal das bisher erratene Geheimtextalphabet:

Klartextalphabet:	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
Geheimtextalphabet:	V	E		S	U	C	H	I	J		L		N	O		Q		W	X	Y	Z		B			G

Da wir wissen, dass es sich um eine Schlüsselwortchiffre handelt, können wir Teile des Geheimtextalphabets auffüllen:

Klartextalphabet:	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
Geheimtextalphabet:	V	E		S	U	C	H	I	J	**K**	L	**M**	N	O	**P**	Q		W	X	Y	Z	**A**	B			G

Man kann auch schon das Schlüsselwort erkennen: VERSUCH. Wir vervollständigen das Geheimtextalphabet:

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

Und erhalten den Klartext:

Seit dem Ende des neunzehnten Jahrhunderts, vereinzelt schon seit der Antike, wird die Mathematik in Form von Theorien praesentiert, die mit Aussagen beginnen, welche als wahr angesehen werden; daraus werden dann weitere wahre Aussagen hergeleitet. Diese Herleitung geschieht dabei nach genau festgelegten Schlussregeln. Die Aussagen, mit denen die Theorie anfaengt, nennt man Axiome, die daraus hergeleiteten nennt man Saetze. Die Herleitung selbst ist ein Beweis des Satzes. In der Praxis spielen noch Definitionen eine Rolle, sie gehoeren aber zum Handwerkszeug der Logik, das vorausgesetzt wird. Aufgrund dieses Aufbaus der mathematischen Theorien bezeichnet man sie als axiomatische Theorien.

Aus http://de.wikipedia.org/wiki/Mathematik

Kommentar:

Um einen Text mittels Häufigkeitsanalyse zu entschlüsseln, benötigt man in der Regel relativ viel Zeit. Da Zeit im Unterricht meistens recht knapp ist, kann darauf verzichtet werden, tatsächlich einen kompletten Text zu knacken. Falls dies doch gemacht wird, sollte auf jeden Fall ein Computerprogramm verwendet werden, um Buchstaben, Bigramme, usw. zu zählen. Hier bietet sich eventuell ein gemeinsames Projekt mit dem Fach Informatik an.

2.2.5. Verschleierung der Häufigkeiten

Um eine unbefugte Entschlüsselung mittels Häufigkeitsanalyse unmöglich zu machen, muss man dafür sorgen, dass alle Geheimtextbuchstaben (bzw. Geheimtextzeichen) gleich häufig auftreten. Dies kann man mit einer **homophonen Verschlüsselung** erreichen.

Bei einer homophonen monoalphabetischen Substitution wird jedem Klartextbuchstaben nicht nur ein Geheimtextzeichen (wie bei der einfachen monoalphabetischen Substitution) zugeordnet, sondern ein Klartextzeichen kann durch mehrere Geheimtextzeichen substituiert werden. D.h. verschiedene Geheimtextzeichen können für denselben Klartextbuchstaben stehen. Trotzdem muss die Zuordnung eindeutig sein, um eindeutiges Dechiffrieren möglich zu machen.

Ordnet man nun den häufiger vorkommenden Klartextbuchstaben mehrere verschiedene Geheimtextzeichen und den seltener auftretenden Klartextbuchstaben nur ein oder wenige Geheimtextzeichen zu, erreicht man, dass alle Geheimtextzeichen mit annähernd gleicher Häufigkeit vorkommen – und das macht eine Entschlüsselung mittels Häufigkeitsanalyse wesentlich schwieriger.

Natürlich könnte die Häufigkeitsanalyse auch auf Bigramme, Trigramme,… ausgeweitet werden, mögliche Angriffspunkte wären charakteristische Bigramme wie CH, CK oder QU und die Reversen EI und IE,… Dazu braucht man aber längere Geheimtexte, als bei der Häufigkeitsanalyse einer einfachen monoalphabetischen Chiffre.

Man kann sagen, dass ein relativ kurzer homophon verschlüsselter Text gegen unbefugtes Entschlüsseln ziemlich gut geschützt ist!

Ein Beispiel:
Um die Zeichenhäufigkeiten im Geheimtext anzugleichen, kann man jedem Klartextbuchstaben so viele Geheimtextzeichen zuordnen, wie seiner relativen Häufigkeit in Prozent entspricht. Es kommt z.B. das „e“ mit rund 17% vor, deswegen werden dem „e“ 17 verschiedene Geheimtextzeichen zugeordnet.
Da die Häufigkeiten aller Klartextbuchstaben zusammen 100% betragen, braucht man also 100 Geheimtextzeichen. Im einfachsten Fall verwendet man dazu die Ziffernpaare 00, 01, 02, …,99, z.B.:

Buchstabe	Zugeordnete Zeichen	Buchstabe	Zugeordnete Zeichen
a	10,21,52,59,71	n	30,35,43,62,67,68,72,77,79
b	20,34	o	02,05,82
c	28,06,80	p	31
d	04,19,70,81,87	q	25
e	09,18,33,38,40,42,53,54,55, 60,66,75,85,86,92,93,99	r	17,36,51,69,74,78,83
f	00,41	s	15,26,45,56,61,73,96
g	08,12,97	t	13,32,90,91,95,98
h	07,24,47,89	u	29,01,58
i	14,39,46,50,65,76,88,94	v	37
j	57	w	22
k	23	x	44
l	16,03,84	y	48
m	27,11,49	z	64

Tabelle aus Albrecht Beutelspacher: Kryptologie, 7.Auflage, Seite 28

Beim Chiffrieren ordnet man einem Klartextbuchstaben zufällig ein dazugehöriges Geheimtextzeichen zu.

Aufgaben:

1. Entschlüssle mithilfe obiger Chiffriertabelle:

23520127 6429 97845929346663, 04597396 9945 5682 86886200712847 141513!

(aus Albrecht Beutelspacher: Kryptologie, 7.Auflage, Seite 28)

Lösung:
Kaum zu glauben, dass es so einfach ist!

2. Welche Häufigkeiten müssten die Geheimtextzeichen aus obiger Chiffriertabelle in einem langen Geheimtext aufweisen?

Lösung:
In einem hinreichend langen Geheimtext müssten die Zeichen mit je ~1% vorkommen, da es 100 Zeichen gibt, die alle annähernd gleichhäufig vorkommen.

2.2.4. Moderne monoalphabetische Chiffren

Obwohl einfache monoalphabetische Chiffren mittels Häufigkeitsanalyse leicht zu knacken sind, finden monoalphabetische Algorithmen auch heute noch Anwendung. Die populärste monoalphabetische Chiffre ist der DES= Data Encryption Standard, der lange Zeit der Verschlüsselungsstandard der US-Regierung war.

Der DES ist eine Blockchiffre, d.h. der Klartext wird in Blöcke zerlegt, die einzeln verschlüsselt werden. Beim DES beträgt die Blocklänge 64 Bits, er verschlüsselt also keine Buchstaben, sonder binäre Folgen (bestehend aus den Symbolen 0 und 1) der Länge 64.
Der 64 Bit lange Klartextblock wird zuerst mit einer sogenannten Eingangspermutation in zwei Teilblöcke zerlegt. Auf den 56 Bit langen Schlüssel wird ebenfalls eine Permutation angewandt und man erhält einen 48 Bit langen Teilschlüssel. Dann wird der resultierende Teilschlüssel in 16 Verschlüsselungsrunden auf die beiden Teilblöcke angewandt. Die resultierenden Blöcke werden mit der zur Eingangspermutation inversen Ausgangspermutation zu einem 64 Bit langen Geheimtextblock zusammengefügt.
Beim Entschlüsseln werden die einzelnen Rundenschlüssel in umgekehrter Reihenfolge angewandt.

Der DES- Algorithmus wurde von IBM entwickelt und 1975 vollständig veröffentlicht - die Sicherheit eines Kryptosystems soll ja nicht von der Geheimhaltung des Algorithmus abhängen (Prinzip von Kerckhoffs).

Der DES gilt noch immer als guter Algorithmus, jedoch haben viele Wissenschaftler seit seiner Veröffentlichung vor der kurzen Schlüssellänge gewarnt. Die möglichen Schlüssel sind alle binären Folgen aus 56 Bits, also $2^{56} \approx 10^{16}$ verschiedene Schlüssel.
1999 wurde der DES erstmals durch eine vollständige Schlüsselsuche gebrochen. Auf einen Geheimtext wurden alle möglichen Schlüssel angewandt, bis sich ein sinnvoller Klartext ergeben hat, das dauerte mit der damaligen Rechenleistung rund 22 Stunden. Der DES wurde also aufgrund seiner geringen Schlüssellänge (und nicht wegen einer Schwachstelle des Algorithmus) geknackt.

Als Verbesserung des DES wurde der TripleDES entwickelt, bei dem zwei DES-Schlüssel verwendet werden und der DES- Algorithmus dreimal angewandt wird: Zuerst wird der Klartext mit dem ersten Schlüssel verschlüsselt, dann mit dem zweiten Schlüssel entschlüsselt und das Ergebnis noch einmal mit dem ersten Schlüssel verschlüsselt.
Der TripleDES ist heute einer der am häufigsten eingesetzten Verschlüsselungsalgorithmen. Aber auch der DES wird noch verwendet, z.B. bei Geldautomaten.

Der Nachfolger des DES ist der im Jahr 2000 veröffentlichte AES, Advanced Encryption Standard, ebenfalls eine Blockchiffre mit monoalphabetischer Substitution.

2.3. Polyalphabetische Chiffren

Bei polyalphabetischen Chiffren wird ein Klartextbuchstabe nicht immer zum gleichen Geheimtextbuchstaben verschlüsselt. Man verwendet nicht nur ein, sondern mehrere Geheimtextalphabete, zwischen denen man wechselt.

2.3.1. Vigenère- Chiffre

Nachdem die über Jahrhunderte als sicher geglaubte monoalphabetische Substitution durch die Erfindung der Häufigkeitsanalyse geknackt wurde, mussten sich die Kryptographen dieser Zeit anstrengen, um eine neue, bessere Verschlüsselungsmethode zu entwickeln.
Die Ursprünge dieses neuen Verfahrens reichen zurück bis in 15 Jahrhundert. Der italienische Mathematiker, Maler, Komponist, Dichter, Philosoph, Schriftsteller und Architekt Leon Battista Alberti legte den Grundstein für die Polyalphabetische Substitution. Um das Jahr 1460 diskutierte er mit seinem Freund Leonardo Dato, dem Geheimsekretär des Papstes, über Fragen der Kryptographie und schrieb schließlich eine Abhandlung über dieses Thema. Darin schlug er eine neue Form der Verschlüsselung vor: Man sollte zwei oder mehr Geheimtextalphabete verwenden und während der Verschlüsselung zwischen diesen hin- und herspringen. Der Vorteil von diesem Verfahren besteht darin, dass der gleiche Klartextbuchstabe nicht immer mit dem gleichen Geheimtextbuchstaben verschlüsselt wird.

Der französische Diplomat Blaise de Vigenère (geboren 1523) entdeckte die Schriften Albertis und begann, mit diesen Ideen ein neues, mächtiges Chiffriersystem zu entwickeln: die Vigenère-Verschlüsselung, die lange Zeit als „Le Chiffre indéchiffrable“, also „Die unentzifferbare Verschlüsselung“ galt.

Die Stärke der Vigenère- Chiffre besteht darin, dass 26 verschiedene Geheimtextalphabete benutzt werden, um einen Klartext zu verschlüsseln.
Für eine Vigenère- Verschlüsselung benötigt man ein **Schlüsselwort** und das sogenannte **Vigenère- Quadrat**, welches aus alles 26 Verschiebechiffren in natürlicher Reihenfolge besteht:

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	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

Das Schlüsselwort kann jede beliebige Buchstabenfolge sein, etwa WINTER. Man schreibt das Schlüsselwort immer wieder über den Klartext:

Schlüsselwort:	W	I	N	T	E	R	W	I	N	T	E	R	W	I	N	T	E		R	W	I	N	T	E	R	W	I	N	T	E
Klartext:	p	o	l	y	a	l	p	h	a	b	e	t	i	s	c	h	e		s	u	b	s	t	i	t	u	t	i	o	n

Beim Chiffrieren wird jeder Klartextbuchstabe mit Hilfe des darüber stehenden Schlüsselwortbuchstaben verschlüsselt und zwar bestimmt der Schlüsselwortbuchstabe das zu verwendende Geheimtextalphabet:
Um den ersten Klartextbuchstaben, das „p“ zu verschlüsseln, muss man die zum Schlüsselbuchstaben „W“ gehörende Zeile im Vigenère- Quadrat verwenden, d.h. das Geheimtextalphabet, das mit „W“ beginnt.
Praktisch sieht man in der Zeile „W“ nach, was in der Spalte „p“ steht: in diesem Fall wird „p“ zu „L“ chiffriert.

Beim Schlüsselwort WINTER brauchen wir insgesamt diese 6 fettgedruckten Alphabete des Vigenère- Quadrats:

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	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

Insgesamt ergibt sich:

Schlüsselwort:	W	I	N	T	E	R	W	I	N	T	E	R	W	I	N	T	E		R	W	I	N	T	E	R	W	I	N	T	E
Klartext:	p	o	l	y	a	l	p	h	a	b	e	t	i	s	c	h	e		s	u	b	s	t	i	t	u	t	i	o	n
Geheimtext:	**L**	**W**	**Y**	**R**	**E**	**C**	**L**	**P**	**N**	**U**	**I**	**K**	**E**	**A**	**P**	**A**	**I**		**J**	**Q**	**J**	**F**	**M**	**M**	**K**	**Q**	**B**	**V**	**H**	**R**

Der Klartextbuchstabe „l“ wird einmal zu einem „Y“ und einmal zu einem „C“ verschlüsselt, während der Geheimtextbuchstabe „J“ von verschiedenen Klartextbuchstaben, nämlich „s“ und „b“ stammt.
Bei einem Vigenère- verschlüsselten Geheimtext ist die Häufigkeit der Buchstaben viel gleichmäßiger verteilt, als bei einer einfachen monoalphabetischen Substitution. Auch die Anzahl der möglichen Schlüssel ist enorm, da jedes Wort, aber auch ganze Sätze verwendet werden können. Das bereitet einem Kryptoanalytiker schon wesentlich größere Schwierigkeiten als eine monoalphabetische Chiffre, doch es macht eine Kryptoanalyse nicht unmöglich…

Aufgaben:

1. Sollte man besser ein kurzes oder ein langes Schlüsselwort bei der Vigenère- Verschlüsselung verwenden?

Lösung:
Ein langes Schlüsselwort ist besser, da bei einem kurzen Schlüsselwort die Gefahr besteht, dass ein Klartextbuchstabe sehr oft durch den gleichen Geheimtextbuchstaben verschlüsselt wird.

2. Entschlüssle folgenden Geheimtext mit dem Schlüsselwort LICHT!
E Z W W I P V C I S F O E H V S W U A X Y

Lösung:
truppenabzug nach osten

3. Verschlüssle eine kurze Nachricht mit der Vigenère- Chiffre! Tausche mit deinem Tischnachbarn Geheimtext und Schlüssel aus und entschlüssle seine Nachricht!

4. Verschlüssle deinen vollen Namen mit dem Schlüsselwort MATHEMATIK!

5. Entschlüssle folgenden Text mit dem Schlüsselwort KROKODIL:

OJKKFHQY WRZOWQSC YBCNWOLL CNOBIUIW DLBNKXAD DVJSSOLP XKWOFHVL
VCSXBDPF XUTOFQMC JRSRZWMP CJSSBZQD CVBQSUVO KBOWSLVU EEUOFGIN
RJRKVHZF XUGMVUQP NVWXVLZY SJHWWUHF VVSBWFPH OZGCSVJP CJSBVDJD
DLRSSUBX KTVNWFPG YDOMYHZW YJYKDLMC DUOCYUWV YUWVXHLZ MYKKFZMT
CVSCGFPW SWTNWHHL OYBOGLKS QRBJZHQD OLBNCKVP XFQRADTH KJNEGDOP
XMSBGFPH KERNSULL MYGSBGMD CVBWOJMY

Lösung:

ESWAREIN MALEINKR OKODILDA SWARURAL TUNDWUSS TEVIELDE NTIERENA
LLENNAHU NDFERNER ZAEHLTEE SSEINWIS SENGERND AKAMEINJ UNGERDAC
HSDAHERU NDSCHRIE DEINHIRN ISTMIRZU LEERICHW EISSESBE SSERHABS
TUDIERTM ACHDICHV OMACKERL OSKAPIER TDASKROK ODILJEDO CHWARWEI
SEESSCHL IFFDIEZA EHNESICH GANZLEIS EUNDOHNE NOCHMALW ASZUSAGE
NVERSCHW ANDDERDA CHSINDES SENMAGEN

Das Krokodil und der Dachs von Helga Kurowski

Es war einmal ein Krokodil
das war uralt und wusste viel.
Den Tieren allen, nah und fern,
erzählte es sein Wissen gern.

Da kam ein junger Dachs daher
und schrie: ,,Dein Hirn ist mir zu leer!
Ich weiß es besser, hab' studiert!
Mach Dich vom Acker! Los!! - Kapiert!!!"

Das Krokodil jedoch war weise,
es schliff die Zähne sich ganz leise.
Und ohne noch mal was zu sagen,
verschwand der Dachs in dessen Magen!

Aus http://www.e-stories.de/gedichte-lesen.phtml?72197

6. Entschlüssle folgenden Text mit dem Schlüsselwort MATHEMATIK:

SLXPG TEKPY QHXSE QNZML DEBAI DEVPD SEPPR
WEEBT QDXZI UTXHO UGMKI EWNMB REEZO XAKMP
ARFRP MRXAW MSLBR PKEIB QNHYQ IEBBO ZTYLV
ZTOWW DANTH QRDCQ QLWPI PEFPS YMXSD GVXZQ
XEBJL QNLQX PDXZA GEKNO XSDHR FEGMM WEGNE
ZZNVN SAKLM ZIKLS ECAGI UCAMX POVOH UEEIC
FDXYI DDXVC OHPLV QILBN QSELF QNLJO ETXYX
QIEQC FDXZQ QNLKR QNULW FEEMR DENUH MMXVN
QANJL EEBVR QIE

Lösung:

Am besten, man schreibt zuerst den Geheimtext in Spalten der Länge 10 (Länge des Schlüsselworts).

```
SLXPGTEKPY QHXSEQNZML DEBAIDEVPD SEPPRWEEBT
QDXZIUTXHO UGMKIEWNMB REEZOXAKMP ARFRPMRXAW
MSLBRPKEIB QNHYQIEBBO ZTYLVZTOWW DANTHQRDCQ
QLWPIPEFPS YMXSDGVXZQ XEBJLQNLQX PDXZAGEKNO
XSDHRFEGMM WEGNEZZNVN SAKLMZIKLS ECAGIUCAMX
POVOHUEEIC FDXYIDDXVC OHPLVQILBN QSELFQNLJO
ETXYXQIEQC FDXZQQNLKR QNULWFEEMR DENUHMMXVN
QANJLEEBVR QIE
```

Man erhält den Klartext:

```
GLEICHERHO EHELAENGEB REITERECHT GEWINKELTJ
```

```
EDESEITEZE IGTDESWUER FELSKLAREF ORMKLARESM
ASSUNDKLAR ENORMWEITE NTFERNTVOM RAUMDERKUG
ELDIEDEMHI MMELZUVERG LEICHENSIN DDESWUERFE
LSKANTENEC KENGANZUND GAREINIRDI SCHZEICHEN
DOCHDIELAS TDERERDENS CHWEREISTD ESLEBENSBE
STERTEILIS TDESMENSCH ENBESTELEH REUNDAMEND
EAUCHSEINH EIL
```

Der Würfel

Gleicher Höhe, Länge, Breite,
rechtgewinkelt jede Seite,
zeigt des Würfels klare Form
klares Maß und klare Norm.
Weit entfernt vom Raum der Kugel,
die dem Himmel zu vergleichen,
sind des Würfels Kanten, Ecken
ganz und gar ein irdisch Zeichen.
Doch die Last der Erdenschwere
ist des Lebens bester Teil,
ist des Menschen beste Lehre
und am Ende auch sein Heil.

Von: Ernst Bühler

Aus http://www.realschule-im-ghz.de/matheged.html

Kommentar:

Die Vigenère- Verschlüsselung ist zwar nicht schwierig zu verstehen, jedoch braucht man dabei zum Ver- und Entschlüsseln ziemlich viel Konzentration. Das könnte einigen Schülern schnell zu mühsam oder zu langweilig werden. Deswegen sollte man (außer die Schüler schreiben und lesen wirklich begeistert Geheimbotschaften) hier nicht zu viele Texte ver- oder entschlüsseln lassen.
Es hilft beim Chiffrieren und auch beim Dechiffrieren, wenn man den Text in Blöcke zusammenfasst, die so lang wie das Schlüsselwort sind, dann muss man nicht zig Mal das Schlüsselwort über den Text schreiben, kann aber nicht so schnell „den Faden verlieren“ und behält besser im Überblick, mit welchem

Schlüsselwortbuchstaben gerade chiffriert (oder dechiffriert) wird.
Bei einem längeren Text wie bei Aufgabe 5 kann man den Text auch aufteilen, damit das Entschlüsseln nicht so langwierig ist.
Wenn man fragt wie man den Text am besten aufteilt, kommt ja vielleicht sogar ein Schüler auf die Idee, den Text nicht einfach zu halbieren oder dritteln,… sondern ihn so aufzuteilen, dass eine Gruppe oder Person immer die ersten Buchstaben einer Spalte, eine andere Gruppe/ Person die zweiten Buchstaben einer Spalte, usw. dechiffriert, denn dann muss jede Gruppe oder Person nur ein einziges Geheimtextalphabet verwenden. Diese Überlegung ist nämlich auch ein wichtiger Teil der Kryptoanalyse von Vigenère- verschlüsselten Texten…

2.3.2. Kryptoanalyse der Vigenère- Chiffre

Bis ins 19. Jahrhundert galt die Vigenère- Verschlüsselung als die „unentzifferbare Verschlüsselung". Als die meisten Kryptoanalytiker den Versuch, die Chiffre zu brechen, schon aufgegeben hatten, versuchte das britische Genie Charles Babbage – angestachelt durch einen Streit mit einem Zeitgenossen- einen Schwachpunkt in der Vigenère- Verschlüsselung zu finden. Er entwickelte vermutlich 1854 eine Methode, die Rückschlüsse auf die Schlüsselwortlänge zulässt und es damit auch möglich macht, die Vigenère- Chiffre zu brechen.
Babbages Entdeckung fand allerdings keine Anerkennung, da er sie nie veröffentlicht hatte. Erst im 20.Jahrhundert fand man heraus, dass schon Babbage eine Methode entwickelt hatte um die Vigenère- Verschlüsselung zu brechen, als Gelehrte seinen Nahlass sichteten. Inzwischen war dieses Verfahren unabhängig davon von Friedrich Willhelm Kasiski entdeckt. Seit er es 1863 in seinem Werk „Die Geheimschriften und die Dechiffrierkunst" veröffentlichte, wird das Verfahren als Kasiski- Test bezeichnet.

Ein ausreichend langer Vigenère- verschlüsselter Geheimtext weist genügend Regelmäßigkeiten auf, um einen Ansatzpunkt zum Brechen dieser Verschlüsselung zu liefern.

Ein Beispiel eines Vigenère- verschlüsselten Geheimtextes:

(aus Albrecht Beutelspacher: Kryptologie, 7.Auflage)

```
EYRYC FWLJH FHSIU BHMJO UCSEG
TNEER FLJLV SXMVY SSTKC MIKZS
JHZVB FXMXK PMMVW OZSIA FCRVF
TNERH MCGYS OVYVF PNEVH JAOVW
UUYJU FOISH XOVUS FMKRP TWLCI

FMWVZ TYOIS UUIIS ECIZV ZVYVF
PCQUC HYRGO MUWKV BNXVB VHHWI
FLMYF FNEVH JAOVW ULYER AYLER
VEEKS OCQDC OUXSS LUQVB FMALF
EYHRT VYVXS TIVXH EUWJG JYARS

ILIER JBVVF BLFVW UHMTV UAIJH
PYVKK VLHVB TCIUI SZXVB JBVVP
VYVFG BVIIO VWLEW DBXMS SFEJG
FHFVJ PLWZS FCRVU FMXVZ MNIRI
GAESS HYPFS TNLRH UYR
```

Es gibt zwei Methoden, um die Schlüsselwortlänge zu bestimmen:

I. Der Kasiski- Test

Grundlage des Kasiski- Tests ist folgende Idee: Wenn im Klartext zwei Folgen aus gleichen Buchstaben auftreten, sind im Allgemeinen die entsprechenden Folgen im Geheimtext verschieden. Es kann aber auch passieren, dass die Anfangsbuchstaben der beiden Klartextfolgen (und damit auch die weitern Buchstaben) mit demselben Schlüsselwortbuchstaben verschlüsselt werden, dann sind auch die entsprechenden Geheimtextfolgen gleich.

Besonders bei einer im Klartext oft vorkommenden Buchstabenfolge, z.B. „ein“ wird es ein paar Mal passieren, dass sie gleich verschlüsselt wird. Das passiert aber nur dann, wenn zwischen die zwei Klartextfolgen das Schlüsselwort genau einmal, zweimal, dreimal,… hineinpasst, d.h. wenn der Abstand der beiden Klartextfolgen ein Vielfaches der Schlüsselwortlänge ist.

Ein Beispiel:

```
Schlüsselwort: W I N T E R W I N T E R W I N
Klartext:      . . . e i n . . . . e i n . .
Geheimtext:    . . . X M E . . . . I Z J . .
```

Im Allgemeinen wird die Klartextfolge „ein“ in verschiedene Geheimtextfolgen chiffriert.

Schlüsselwort: W I N T E R W I N T E R W I N
Klartext: . . e i n . . . e i n . . . .
Geheimtext: . . R B R . . . R B R . . . .

Wenn aber die Anfangsbuchstaben der Folgen unter dem gleichen Schlüsselwortbuchstaben stehen, denn sind auch die entsprechenden Geheimtextfolgen gleich.
Also werden zwei gleiche Klartextfolgen genau dann in gleiche Geheimtextfolgen verschlüsselt, wenn ihr Abstand ein Vielfaches der Schlüsselwortlänge ist. Mit diesem Ansatz kann man die Schlüsselwortlänge bestimmten.

Gleiche Geheimtextfolgen können also zufällig entstehen, wahrscheinlicher ist es aber bei Folgen von drei oder mehr gleichen Buchstaben, dass sie aus gleichen Klartextfolgen hervorgehen. Findet man im Geheimtext solche gleichen Buchstabenfolgen, geht man davon aus, dass ihr Abstand ein Vielfaches der Schlüsselwortlänge ist.

Voriges Beispiel mit hervorgehobenen gleichen Buchstabenfolgen:

EYRYC FWLJH FHSIU BHMJO UCSEG
TNEER FLJLV SXMVY SSTKC MIKZS
JHZVB FXMXK PMMVW OZSIA **FCRV**F
TNERH MCGYS OVYVF PNEVH JAOVW
UUYJU F***OIS***H XOVUS FMKRP TWLCI

FMWVZ TY***OIS*** UUIIS ECIZV ZVYVF
PCQUC HYRGO MUWKV BNXVB VHHWI
FLMYF F**NEVH JAOVW U**LYER AYLER
VEEKS OCQDC OUXSS LUQVB FMALF
EYHRT VYVXS TIVXH EUWJG JYARS

ILIER JBVVF BLFVW UHMTV UAIJH
PYVKK VLHVB TCIUI SZXVB JBVVP
VYVFG BVIIO VWLEW DBXMS SFEJG
FHFVJ PLWZS **FCRV**U FMXVZ MNIRI
GAESS HYPFS TNLRH UYR

Man erhält:

Buchstabenfolge	Abstand	Primfaktorenzerlegung
TNE	50	2.5.5
FCRV	265	5.53
NEVHAJAOVWU	90	2.3.3.5
VWU	90	2.3.3.5.
VWU	75	3.5.5
OIS	*26*	*2.13*

Die Buchstabenfolge OIS hat als einzige keinen durch 5 teilbaren Abstand, sie ist wahrscheinlich zufällig entstanden. Der größte gemeinsame Faktor der anderen Folgen ist 5, dies ist ein starkes Indiz dafür, dass die Schlüsselwortlänge 5 oder ein Vielfaches von 5 ist.

Der Kasiski- Test liefert also die Schlüsselwortlänge bis auf Vielfache oder Teiler.

II. Der Friedman- Test

Diese Methode liefert eine Größenordnung der Schlüsselwortlänge, sie wurde 1925 von Willhelm Friedman entwickelt. Die Grundidee dieses Testes ist, dass der **Koinzidenzindex** eines Textes, der die Wahrscheinlichkeit angibt, mit der zwei zufällig herausgegriffene Buchstaben gleich sind, bei einem monoalphabetisch und einem polyalphabetisch chiffrierten Text unterschiedlich ist. Bei einer polyalphabetischen Chiffrierung hängt er sogar von der Schlüsselwortlänge ab und so kann man, wenn man den Koinzidenzindex kennt, auf die ungefähre Länge des Schlüsselwortes schließen.

Berechnung des Koinzidenzindex:

Sei bei einer beliebigen Buchstabenfolge der Länge n die Anzahl der a's gleich n_1, die Anzahl der b's gleich n_2,… und die Anzahl der z's gleich n_{26}.

Die Anzahl der Buchstabenpaare (es müssen keine aufeinanderfolgenden Buchstaben sein), bei denen beide Buchstaben gleich a sind, ist $\frac{n_1 \cdot (n_1 - 1)}{2}$, weil:

Für die Auswahl des ersten a's gibt es genau n_1 Möglichkeiten und für die Auswahl des zweiten a's noch n_1-1 Möglichkeiten, also $n_1.(n_1\text{-}1)$ mögliche Kombinationen. Da aber die Reihenfolge der Buchstaben egal ist, ist die Anzahl der Paare nur die Hälfte,

also $\frac{n_1 \cdot (n_1 - 1)}{2}$.

Die Anzahl der Paare, bei denen beide Buchstaben gleich sind, d.h. beide Buchstaben gleich a oder beide gleich b … oder beide gleich c, ist demnach

$$\frac{n_1 \cdot (n_1 - 1)}{2} + \frac{n_2 \cdot (n_2 - 1)}{2} + \ldots + \frac{n_{26} \cdot (n_{26} - 1)}{2} = \sum_{i=1}^{26} \frac{n_i . (n_i - 1)}{2}.$$

Die Wahrscheinlichkeit, so ein Paar aus gleichen Buchstaben zu erwischen, lässt sich nach der Methode „Anzahl der Günstigen durch Anzahl der Möglichen" berechnen, also

$$\frac{\sum_{i=1}^{26} \frac{n_i . (n_i - 1)}{2}}{\frac{n \cdot (n-1)}{2}} = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)}.$$

Diese Zahl heißt (Friedmann'scher) Koinzidenzindex und wird mit I bezeichnet:

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)}$$

Der Koinzidenzindex lässt sich aber auch mit Hilfe der Buchstabenhäufigkeiten berechnen:
In einem Text kommt jeder Buchstabe mit einer bestimmten Wahrscheinlichkeit p_i vor, also der Buchstabe a mit Wahrscheinlichkeit p_1, b mit Wahrscheinlichkeit p_2,…und z mit Wahrscheinlichkeit p_{26}.
Wenn man nun ein Buchstabenpaar zufällig auswählt, dann ist die Wahrscheinlichkeit dass man beim ersten Mal ein a erwischt gleich p_1, die

Wahrscheinlichkeit, dass der zweite Buchstabe ein a ist, ist wieder p_1, also ist die Wahrscheinlichkeit, dass beide Buchstaben ein a sind gleich p_1. $p_1 = p_1^2$.
Das gilt auch für die anderen Buchstaben, somit ist die Wahrscheinlichkeit, dass ein zufällig gewähltes Buchstabenpaar aus zwei gleichen Buchstaben besteht (also zwei a's oder zwei b's… oder zwei z's) gleich

$p_1^2 + p_2^2 + \ldots + p_{26}^2 = \sum_{i=1}^{26} p_i^2$, d.h. $\quad I = \sum_{i=1}^{26} p_i^2$

Wenn man also die Wahrscheinlichkeiten der Buchstaben kennt, kann man den Koinzidenzindex im Vorhinein ausrechnen.

Der **Koinzidenzindex der deutschen Sprache**, von der man die Buchstabenhäufigkeiten kennt (siehe Tabelle im Kapitel 2.2.2), ist

$$\sum_{i=1}^{26} p_i^2 = 0{,}0651^2 + 0{,}0189^2 + 0{,}0306^2 + \ldots + 0{,}0113^2 = 0{,}0762.$$

Der Koinzidenzindex der deutschen Sprache ist 0,0762, das bedeutet, dass ein zufällig gewähltes Buchstabenpaar mit 7,62%-iger Wahrscheinlichkeit aus gleichen Buchstaben besteht. D.h. etwa jedes dreizehnte Buchstabenpaar besteht aus gleichen Buchstaben.

Der **Koinzidenzindex einer zufälligen Buchstabenfolge**, bei der die Buchstabenhäufigkeiten gleichverteilt sind, also jeder Buchstabe mit der Wahrscheinlichkeit $1/26 \approx 0{,}0385$ vorkommt, ist

$$\sum_{i=1}^{26} p_i^2 = \sum_{i=1}^{26} \left(\frac{1}{26}\right)^2 = 26. \ \frac{1}{26^2} = \frac{1}{26} \approx 0{,}0385.$$

Hier besteht nur etwa jedes sechsundzwanzigste Buchstabenpaar aus gleichen Buchstaben.

Der Koinzidenzindex ist also größer, wenn der Text unregelmäßig ist, und kleiner, wenn der Text gleichmäßig ist. Da es nur 26 Buchstaben gibt, kann der Koinzidenzindex nicht kleiner als $1/26 \approx 0{,}0385$ sein, wie vorher für die zufällige Buchstabenfolge gezeigt wurde.

Da bei einer monoalphabetischen Chiffre die verschiedenen Buchstabenhäufigkeiten erhalten bleiben (nur anderen Buchstaben zugeordnet), sollte auch der Koinzidenzindex eines monoalphabetisch chiffrierten Textes bei ungefähr 0,0762 liegen. Bei einem polyalphabetisch chiffrierten Text sinkt der Koinzidenzindex, weil bei einer Polyalphabetischen Substitution die Buchstabenhäufigkeiten angeglichen werden.

Mit Hilfe der Koinzidenzindex kann man also testen, ob ein Geheimtext monoalphabetisch verschlüsselt wurde.

Berechnung der Schlüsselwortlänge:
Um die Länge des Schlüsselwortes herauszufinden, nimmt man an, die Schlüsselwortlänge zu kennen und berechnet daraus den Koinzidenzindex. Man erhält eine Formel für den Koinzidenzindex, die von der Schlüsselwortlänge abhängig ist. Dann kann man den Koinzidenzindex des Geheimtextes (mittels Buchstabenhäufigkeiten) berechnen und die Formel einsetzen, um die Schlüsselwortlänge zu bekommen.

Sei h die Länge des Schlüsselworts, d.h. die Anzahl seiner Buchstaben. Dann sind die Geheimtextbuchstaben Nummer 1, h+1, 2h+1, 3h+1,… mit dem ersten Schlüsselwortbuchstaben verschlüsselt worden. Ebenso sind die Buchstaben Nummer 2, h+2, 2h+2,… mit dem zweiten Schlüsselwortbuchstaben verschlüsselt worden.

Nun schreibt man den Geheimtext zeilenweise in h Spalten, somit befinden sich alle Buchstaben, die mit demselben Schlüsselwortbuchstaben chiffriert wurden in einer Spalte:

Erster Schlüsselwort-buchstabe	Zweiter Schlüsselwort-buchstabe	Dritter Schlüsselwort-buchstabe	…	h-ter Schlüsselwort-buchstabe
1	2	3	…	h
h+1	h+2	h+3	…	2h
2h+1	2h+2	2h+3	…	3h
3h+1	3h+2	3h+3	…	4h
…	…	…	…	…

Wahrscheinlichkeiten der Buchstabenpaare:

In jeder Spalte stehen Buchstaben, die mit derselben monoalphabetischen Chiffre verschlüsselt wurden, d.h. die Wahrscheinlichkeit, in einer Spalte auf ein Paar aus gleichen Buchstaben zu treffen, ist 0,0762.
Wenn das Schlüsselwort eine zufällige Buchstabenfolge ist, dann wurden die Buchstaben aus verschiedenen Spalten mit Verschlüsselungsalphabeten chiffriert, die zufällig gewählt wurden. Das heißt, ein Buchstabenpaar aus verschiedenen Spalten kann nur zufällig aus gleichen Buchstaben bestehen und die Wahrscheinlichkeit dafür ist 0,0385.

Anzahlen der Buchstabenpaare:

Wenn der Geheimtext aus insgesamt n Buchstaben besteht, dann stehen in jeder Spalte n/h Buchstaben.
Es gibt n Möglichkeiten, einen bestimmten Buchstaben aus dem Geheimtext zu wählen. In derselben Spalte gibt es dann noch n/h -1 andere Buchstaben, d.h. n/h -1 Möglichkeiten, einen zweiten Buchstaben aus dieser Spalte zu wählen. Es gibt also n.(n/h -1) mögliche Buchstabenpaare. Da die Reihenfolge der Buchstaben egal ist, ist die Anzahl der Paare, die sich in der gleichen Spalte befinden also

$$\frac{n\cdot\left(\frac{n}{h}-1\right)}{2}=\frac{n\cdot(n-h)}{2h}.$$

Wenn man einen der n Geheimtextbuchstaben auswählt, dann gibt es noch n- n/h Buchstaben in anderen Spalten. Also ist die Anzahl der Paare, die sich in verschiedenen Spalten befinden gleich

$$\frac{n\cdot\left(n-\frac{n}{h}\right)}{2}=\frac{n^2\cdot(h-1)}{2h}.$$

Die erwartete Anzahl von Paaren aus gleichen Buchstaben ist $\frac{n\cdot(n-h)}{2h}$. 0,0762 mit Buchstaben aus derselben Spalte und $\frac{n^2\cdot(h-1)}{2h}$. 0,0385 mit Buchstaben aus verschiedenen Spalten, also insgesamt erwartet man

A = $\frac{n\cdot(n-h)}{2h}$. 0,0762 + $\frac{n^2\cdot(h-1)}{2h}$. 0,0385 Buchstabepaare aus gleichen Buchstaben.

Insgesamt gibt es $\frac{n\cdot(n-1)}{2}$ mögliche Buchstabenpaare, d.h. die Wahrscheinlichkeit, auf ein Paar aus gleichen Buchstaben zu treffen ist („Günstige durch Mögliche“)

$$\frac{A}{\frac{n\cdot(n-1)}{2}}=\frac{\frac{n\cdot(n-h)}{2h}.0{,}0762+\frac{n^2\cdot(h-1)}{2h}.0.0385}{\frac{n\cdot(n-1)}{2}}=\frac{(n-h).0{,}0762+n.(h-1).0{,}0385}{h.(n-1)}=$$

$$=\frac{0{,}0377.n+h.(0{,}0385n-0{,}0762)}{h.(n-1)}=\frac{0{,}0377n}{h.(n-1)}+\frac{0{,}0385n-0{,}0762}{n-1}.$$

Und da der Koinzidenzindex eben die Wahrscheinlichkeit, auf ein Paar aus gleichen Buchstaben zu treffen angibt, ist

$$I=\frac{0{,}0377n}{h.(n-1)}+\frac{0{,}0385n-0{,}0762}{n-1}$$

Durch Umformen erhält man eine Formel für die Länge h des Schlüsselworts:

$$h=\frac{0{,}0377n}{I.(n-1)-0{,}0385n+0{,}0762}$$

Ein Beispiel:

Wendet man diese Formel beim obigen Beispiel (Anfang dieses Kapitels) an, dann ergibt sich n=368 und

i	n_i	$n_i.(n_i-1)$	i	n_i	$n_i.(n_i-1)$	i	n_i	$n_i.(n_i-1)$
1	8	56	10	14	182	19	24	552
2	12	132	11	8	56	20	10	90
3	13	156	12	15	210	21	19	342
4	2	2	13	16	240	22	41	1640
5	18	306	14	7	42	23	13	156
6	25	600	15	12	132	24	11	110
7	7	42	16	8	56	25	19	342
8	19	342	17	3	6	26	9	72
9	20	380	18	15	210			

$$\sum_{i=1}^{26} n_i.(n_i-1) = 6454$$

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i-1)}{n \cdot (n-1)} = \frac{6454}{368.367} = \frac{6454}{135056} \approx 0{,}04779$$

=> Es handelt sich also sehr wahrscheinlich um einen polyalphabetisch verschlüsselten Text.

$$h = \frac{0{,}0377n}{I.(n-1) - 0{,}0385n + 0{,}0762} = \frac{0{,}0377.368}{0{,}04779.367 - 0{,}0385.368 + 0{,}0762} \approx 4{,}025$$

=> Dies deutet zusammen mit dem Kasiski- Test (Schlüsselwortlänge 5 oder ein Vielfaches) darauf hin, dass die Schlüsselwortlänge tatsächlich 5 ist.

Der Kasiski- Test liefert also einen Richtwert für die Größenordnung der Schlüsselwortlänge.

III. Bestimmung des Schlüsselworts

Kennt man nun die Länge h des Schlüsselworts, dann weiß man, dass die Geheimtextbuchstaben, die in der Tabelle unter dem ersten Schlüsselbuchstaben stehen (also die Buchstaben Nummer 1, h+1, 2h+1,…) bzw. die Geheimtextbuchstaben, die unter dem zweiten Schlüsselwortbuchstaben stehen (also Nummer 2, h+2, 2h+2,…) u.s.w. jeweils mit derselben monoalphabetischen Chiffre verschlüsselt wurden. D.h. man kann jede Spalte als eigene monoalphabetische Chiffre betrachten und entschlüsseln.
Da es sich bei der Vigenère- Verschlüsselung nur um Verschiebechiffren handelt, ist es nun relativ leicht, die jeweiligen Verschiebechiffren herauszufinden. Dazu genügt es meistens, in jeder Spalte den häufigsten Buchstaben, also das Geheimtextäquivalent zu „e“, zu finden. Dadurch weiß man, um welche Verschiebechiffre es sich handelt, und kennt den jeweiligen Schlüsselwortbuchstaben.

Voriges Beispiel:

```
EYRYC FWLJH FHSIU BHMJO UCSEG
TNEER FLJLV SXMVY SSTKC MIKZS
JHZVB FXMXK PMMVW OZSIA FCRVF
TNERH MCGYS OVYVF PNEVH JAOVW
UUYJU FOISH XOVUS FMKRP TWLCI

FMWVZ TYOIS UUIIS ECIZV ZVYVF
PCQUC HYRGO MUWKV BNXVB VHHWI
FLMYF FNEVH JAOVW ULYER AYLER
VEEKS OCQDC OUXSS LUQVB FMALF
EYHRT VYVXS TIVXH EUWJG JYARS

ILIER JBVVF BLFVW UHMTV UAIJH
PYVKK VLHVB TCIUI SZXVB JBVVP
VYVFG BVIIO VWLEW DBXMS SFEJG
FHFVJ PLWZS FCRVU FMXVZ MNIRI
GAESS HYPFS TNLRH UYR
```

Im obigen Beispiel ist h=5. Bei den 74 Buchstaben der ersten Verschiebechiffre (also der ersten Spalte, d.h. jeder fünfte Buchstabe) tritt am häufigsten, und zwar 13 Mal, das F auf, daher entspricht F dem Klartextbuchstaben e.

Wenn man im Vigenère- Quadrat überprüft, bei welchem Geheimtextalphabet das e zu einem F verschlüsselt wird (indem man in der Spalte e nachsieht, in welcher Zeile ein F steht), erkennt man, dass der erste Schlüsselbuchstabe ein **B** sein muss.
In der zweiten Spalte kommt der Buchstabe Y mit 11 Mal am häufigsten vor, also ist der zweite Schlüsselwortbuchstabe ein **U**. Bei der dritten Verschiebchiffre tritt I 8 Mal, E 7 Mal und V 7 Mal auf, in diesem Fall ist es nicht ganz eindeutig: der nächste Schlüsselwortbuchstabe ist ein **E, A oder R.** In der Vierten Spalte kommt das V 21 Mal vor und dieser Schlüsselwortbuchstabe ist **R**. In der fünften Spalte findet man 13 Mal das S, also ist der fünfte Schlüsselwortbuchstabe ein **O**.

	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**	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

Mögliche Schlüsselwörter wären demnach BUERO, BUARO oder BURRO. Man wird vermuten, das Schlüsselwort also BUERO lautet und man benötigt folgende Geheimtextalphabete:

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
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
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
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
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

Der Klartext lautet also:

```
DENHO ECHST ENORG ANISA TIONS
STAND ERFUH RDIEK RYPTO LOGIE
INVEN EDIGW OSIEI NFORM EINER
STAAT LICHE NBUER OTAET IGKEI
TAUSG EUEBT WURDE ESGAB SCHLU

ESSEL SEKRE TAERE DIEIH YBUER
OIMDO GENPA LASTH ATTEN UNDFU
ERIHR ETAET IGKEI TRUND ZEHND
UKATE NIMMO NATBE KAMEN ESWUR
DEDAF UERGE SORGT DASSS IEWAE

HREND IHRER ARBEI TNICH TGEST
OERTW URDEN SIEDU RFTEN IHREB
UEROS ABERA UCHNI CHTVE RLASS
ENBEV ORSIE EINEG ESTEL LTEAU
FGABE GELOE STHAT TEN
```

Und mit richtig gesetzten Leerzeichen:

```
DEN HOECHSTEN ORGANISATIONSSTAND ERFUHR DIE KRYPTOLOGIE IN
VENEDIG WO SIE IN FORM EINER STAATLICHEN BUEROTAETIGKEIT
AUSGEUEBT WURDE ES GAB SCHLUESSELSEKRETAERE DIE IHY BUERO IM
DOGENPALAST HATTEN UND FUER IHRE TAETIGKEIT RUND ZEHN DUKATEN
IM MONAT BEKAMEN ES WURDE DAFUER GESORGT DASS SIE WAEHREND
IHRER ARBEIT NICHT GESTOERT WURDEN SIE DURFTEN IHRE BUEROS ABER
AUCH NICHT VERLASSEN BEVOR SIE EINE GESTELLTE AUFGABE GELOEST
HATTEN
```

Verbesserung des Schlüsselworts:

Um trotzdem zu verhindern, dass die Vigenère- Chiffre geknackt werden kann, kann man versuchen, die Bestimmung des Schlüsselworts wesentlich zu erschweren.
Erste Möglichkeit: Man wählt als Schlüsselwort nicht nur ein Wort, sondern einen Text, der mindestens so lang ist wie der zu chiffrierende Klartext. Hier könnte man zum Beispiel ein Buch verwenden: der Schlüssel, also Autor und Titel des Buches (evtl. noch eine Seitenangabe), ist nicht schwierig zu übermitteln bzw. ist leicht zu merken. Bei Verwendung eines solchen „Schlüsselworts“ sind alle Methoden, um die Schlüsselwortlänge zu bestimmen, zwecklos.
Ist aber der Geheimtext (und somit der zugehörige Schlüssel) lang genug, schlagen statistisch erfassbare Daten der Sprache auf den Geheimtext durch und es lassen sich möglicherweise wieder Ansatzpunkte für eine Kryptoanalyse finden.
Zweite Möglichkeit: Man verwendet als Schlüsselwort eine unendlich lange, zufällige Buchstabenfolge, an der alle statistischen Tests scheitern. Verschlüsselt man einen Klartext mit einer solchen Zufallsfolge (auch Buchstabenwurm genannt), weist auch der Geheimtext keine statistischen Ansatzpunkte mehr auf. Der Vorteil eines so

chiffrierten Textes ist, dass man mit einem beliebig langen Stück Geheimtext (sogar mit einem beliebig langen zusammengehörigen Stück Klartext-Geheimtext) keinen einzigen (weiteren) Buchstaben bestimmen kann!

Aufgaben:

1. Bestimme den Koinzidenzindex des Textes aus dem Beispiel in Kapitel 2.2.4.!

PR ISRSQ YSPUD SYOCREBS GPS NFRZB GSY NCYBVEYCWDPS SPRS ZVOUDS HVOONVQQSRDSPB, GCZZ GPS NCYBS SPRSY SPRMPESR WYVHPRM GSR YCFQ SPRSY ECRMSR ZBCGB SPRRCDQ FRG GPS NCYBS GSZ YSPUDZ GSR SPRSY WYVHPRM. QPB GSY MSPB ASTYPSGPEBSR GPSZS FSASYQCSZZPE EYVZZSR NCYBSR PRUDB OCSRESY, FRG QCR SYZBSOOBS SPRS NCYBS GSZ YSPUDZ, GPS ESRCF GPS EYVSZZS GSZ YSPUDZ DCBBS.

AVYESZ, HVR GSY ZBYSRES GSY JPZZSRZUDCTB

Lösung:

S	R	P	Y	Z	B	G	C	E	D	V	Q	O	U	N	F	M	H	W	A	T	I	J	L	K	X
67	32	30	29	24	20	20	18	12	11	10	8	7	7	7	6	5	4	3	3	2	1	1	0	0	0

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)} = \frac{9304}{327.326} = \frac{9304}{106602} \approx 0{,}087$$

Dieser Text ist mit sehr großer Wahrscheinlichkeit monoalphabetisch verschlüsselt.

2. Bestimme den Koinzidenzindex des Textes aus Aufgabe 5 in Kapitel 2.3.1.!

OJKKFHQY WRZOWQSC YBCNWOLL CNOBIUIW DLBNKXAD DVJSSOLP XKWOFHVL VCSXBDPF XUTOFQMC JRSRZWMP CJSSBZQD CVBQSUVO KBOWSLVU EEUOFGIN RJRKVHZF XUGMVUQP NVWXVLZY SJHWWUHF VVSBWFPH OZGCSVJP CJSBVDJD DLRSSUBX KTVNWFPG YDOMYHZW YJYKDLMC DUOCYUWV YUWVXHLZ MYKKFZMT CVSCGFPW SWTNWHHL OYBOGLKS QRBJZHQD OLBNCKVP XFQRADTH KJNEGDOP XMSBGFPH KERNSULL MYGSBGMD CVBWOJMY

Lösung:

S	V	W	O	B	L	C	D	K	U	H	F	J	Y	P	M	G	N
21	20	19	18	16	15	15	15	14	13	13	13	13	13	11	11	10	10

X	Z	Q	R	T	E	I	A
10	10	9	9	5	4	3	2

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)} = \frac{4924}{312.311} = \frac{4924}{97032} \approx 0{,}051$$

Der Text ist mit großer Wahrscheinlichkeit polyalphabetisch verschlüsselt.

3. Bestimme die mögliche Schlüsselwortlänge des folgenden Textes mittels Kasiski- Test!

KWCSS GXYUT ZBZMU CMRFY JZZNZ HMEBS WMEXA ZMZAW
IATBS ABUUK NMZHT ZAKCE HBVLY ZPVCE OMONT PKYML
VJVGW CZRFK ZQEYF FTRLL ZFKVM XPJNS WMEXS MAKYD
GMEES IVRVW MURHV VZWHA XPKPW MOVMK ZVUUK NLVLY
ZPVCE OMONV ZVBFS MBVRL ZQEXW PBZAT ZAKCE HMEGM
NAQOE WMZMH DMCCK OMJHA XPKGG ZOICU CLRMK DMVCF
ZURFY JZZNZ HCJXW MOVBW DUKYP OJLWZ NBRVW IQDED
VZKYP OMZHE VTVOF YMZHS ILVLW NURFK ZVKMH MQTBL
JPEYV VAJYK YIWOW MMZHW MMXYD BQSNV DMUYE ZUGZS
ZVXYJ BMEUM NIXNO VVEYJ ZCEXO VVEYJ NMENK KZZWZ
OMJCK OMENK XPVCV ZVUXS NARHB ZLVLK OMCFW YMJEJ
TXKIY MIDGK YMIMU CTLYK NMCYA ILVOL DOUYF FTRLL
ZFKVM XPJNS WMETM EMUYE BMYYA HBVRL WCTBK OISYF
AMJND ZOK

Lösung:

KWCSS GXYUT ZBZMU CMRFY JZZNZ HMEBS WMEXA ZMZAW
IATBS AB**UUK** NMZHT ZAKCE HBVLY ZPVCE OMONT PKYML
VJVGW CZRFK ZQE**YF FTRLL ZFKVM XPJNS WME**XS MAKYD
GMEES IVRVW MURHV VZWHA XPKPW MOVMK ZV**UUK** NLVLY
ZPVCE **OMO**NV ZVBFS MBVRL ZQEXW PBZAT ZAKLE HMEGF
NAQOE WMZMH DMICK OMJHA XPKGG ZOICU CLRMK DVVCF
ZURFY JZZNZ HCJXW MOVBW DUKYP OJLWZ NBRVW SQDED
VZKYP OMZHE VTVOF YMZHS ILVLW NURFK ZVKMH MQTBL
JPEYV VAJYK YIWOW MMZHW MMXYD BQSNV DMUYE ZUGZS
ZVXYJ BMEUM NIXNO VVEYJ ZCEXO VVEYJ NMENK KZZWZ
OMJCK OMENK XPVCV ZVUXS NARHB ZLVLK OMIFW YMJEJ
TXKIY MIDGK YMIMU CTLYK NMIYA ILVHL DOU**YF FTRLL**
ZFKVM XPJNS WMENM ENUYE BMYYA HBVRL WCTBK OISYF
AMJND ZOK

Buchstabenfolge	Abstand	Primfaktorenzerlegung
SWMEX	80	2.2.5
UUK	105	3.5.7
OMO	95	5.19
YFFTRLLZFKVMXPJNSWME	380	2.2.5.19
ZVU	265	5.53

Die Schlüsselwortlänge beträgt vermutlich 5.

4. Überprüfe die vermutete Schlüsselwortlänge aus Aufgabe 3 mittels Friedmann- Test!

Lösung:

M	Z	V	K	Y	E	W	O	L	N	C	U	B	J	X	A	H	F	S
52	43	39	30	29	27	22	22	20	20	20	18	17	17	16	16	15	15	14

R	P	T	I	D	G	Q
13	13	13	12	11	8	6

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)} = \frac{13116}{528.527} = \frac{13116}{278256} \approx 0{,}047\,14$$

$$h = \frac{0{,}0377n}{I.(n-1) - 0{,}0385n + 0{,}0762} = \frac{0{,}0377.528}{0{,}04714.527 - 0{,}0385.528 + 0{,}0762} \approx 4{,}336$$

Da h in der Nähe von 5 liegt, wurde die Vermutung von Aufgabe 3 bestätigt.

5. Bestimme das Schlüsselwort des Textes aus Aufgabe 3 und entschlüssle den Text!

Lösung:

Spalte	Häufigster Buchstabe	Schlüsselwort-Buchstabe
1	Z	V
2	M	I
3	V	R
4	Z	U
5	W oder K	S oder G

Das Schlüsselwort lautet VIRUS und ergibt folgenden Klartext:

```
POLYA LPHAB ETISC HEALG ORITH MENHA BENDI EEIGE
NSCHA FTDAS SEINB ESTIM MTERG EHEIM TEXTB UCHST
ABEME HRALS EINEN KLART EXTBU CHSTA BENDA RSTEL
LENKA NNABE RMAND ARFNI CHTVE RGESS ENDAS SDERG
EHEIM TEXTD ENKLA RTEXT EINDE UTIGB ESTIM MENMU
SSZUM BEISP IELIS TESNI CHTMO EGRIC HDASS IEEIN
EMALG ORITH MUSDE RGEHE IMTEX TBUCH STABE NIMKL
ARTEX TEINMA LEUN DEINA NDERE SMALS ENTSP RICHT
OHNED ASSES DAFUE REINE REGEL GIBTD IEDEM EMPFA
ENGER GENAU SAGTW ANNER EUNDW ANNER SENTS PRICH
TESIS TENTS CHEID ENDDA SSANJ EDERS TELLE DESKR
YPTOG RAMMS DERSC HLUES SELEI NDEUT IGDEN KLART
EXTBU CHSTA BENZU JEDEM GEHEI MTEXT BUCHS TABEN
FESTL EGT
```

Mit richtig gesetzten Leerzeichen:

Polyalphabetische Algorithmen haben die Eigenschaft, dass ein bestimmter Geheimtextbuchstabe mehr als einen Klartextbuchstaben darstellen kann. Aber man darf nicht vergessen, dass der Geheimtext den Klartext eindeutig bestimmen muss. Zum Beispiel ist es nicht moeglich, das Sie einem Algorithmus der Geheimtextbuchstaben im Klartext einmal e und ein anderes Mal s entspricht, ohne dass es dafuer eine Regel gibt, die dem Empfaenger genau sagt, wann er e und wann er s entspricht. Es ist entscheidend, dass an jeder Stelle des Kryptogramms der Schluessel eindeutig den Klartextbuchstaben zu jedem Geheimtextbuchstaben festlegt.

6. Führe beim folgenden Text den Kasiski- Test durch und bestimme die vermutliche Schlüsselwortlänge!

```
AXTRX TRYLC TYSZO EMLAF QWEUZ HRKDP NRVWM WXRPI
JTRHN IKMYF WLQIE NNOXW OTVXB NEXRK AFYHW KXAXF
QYAWD PKKWB WLZOF XRLSN AAWUX WTURH RFWLL WWKYF
WGAXG LPCTG ZXWOX RPIYB CSMYF WIKPA DHYBC SMYFW
KGMTE EUWAD LHSLP AVHFK HMWLK
```

Lösung:

Kasiski- Test:

```
AXTRX TRYLC TYSZO EMLAF QWEUZ HRKDP NRVWM WXRPI
JTRHN IKMYF WLQIE NNOXW OTVXB NEXRK AFYHW KXAXF
QYAWD PKKWB WLZOF XRLSN AAWUX WTURH RFWLL WWKYF
WGAXG LPCTG ZXWOX RPIYB CSMYF WIKPA DHYBC SMYFW
KGMTE EUWAD LHSLP AVHFK HMWLK
```

Buchstabenfolge	Abstand	Primfaktorenzerlegung
XTR	3	3
XRPI	98	2.7.7
YFW	70	2.5.7
YBCSMYFW	14	2.7

Da der Faktor 3 nur einmal vorkommt, nimmt man an, dass diese Buchstabenwiederholung nur zufällig entstanden ist.
Die Faktoren 2 und 7 kommen sonst bei allen Abständen vor, also ist die vermutliche Länge des Schlüsselworts 2, 7 oder 14.

7. Die tatsächliche Schlüsselwortlänge des Textes aus Aufgabe 6 ist 14. Überprüfe dies mit dem Friedmann- Test! Wie ist das Ergebnis zu erklären?

Lösung:
Friedmann- Test

W	X	L	A	K	R	F	Y	T	H	P	M	E	N	I	S	O	C	B	Z	D	U	G	Q	V	J
20	13	11	11	11	11	10	10	8	8	7	7	6	6	5	5	5	4	4	4	4	4	4	3	3	1

$$I = \frac{\sum_{i=1}^{26} n_i \cdot (n_i - 1)}{n \cdot (n-1)} = \frac{1556}{185.184} = \frac{1556}{34040} \approx 0{,}04571$$

$$h = \frac{0{,}0377n}{I.(n-1) - 0{,}0385n + 0{,}0762} = \frac{0{,}0377.185}{0{,}04571.184 - 0{,}0385.185 + 0{,}0762} \approx 5{,}112$$

Dieser Wert liegt näher bei 7 als bei 14, obwohl das Schlüsselwort eigentlich 14 Buchstaben hat. Die große Abweichung der errechneten von der tatsächlichen Schlüsselwortlänge lässt sich dadurch erklären, dass der zu analysierende Geheimtext mit weniger als 200 Buchstaben sehr kurz ist. Bei so kurzen Texten haben Zufälle in statistischen Berechnungen große Auswirkung.
Man darf sich also besonders bei kurzen Texten nicht blind auf die Ergebnisse solcher Tests verlassen!

8. Entschlüssle den Text aus Aufgabe 6 mit dem Schlüsselwort ALTESTESTAMENT!

Lösung:

Am besten, man schreibt den Geheimtext zum Entschlüsseln zuerst in Spalten der Länge 14 (Schlüsselwortlänge):

```
AXTRXTRYLCTYSZ OEMLAFQWEUZHRK DPNRVWMWXRPIJT RHNIKMYFWLQIEN
NOXWOTVXBNEXRK AFYHWKXAXFQYAW DPKKWBWLZOFXRL SNAAWUXWTURHRF
WLLWWKYFWGAXGL PCTGZXWOXRPIYB CSMYFWIKPADHYB CSMYFWKGMTEEUW
ADLHSLPAVHFKHM WLK
```

Der Klartext lautet:

```
AMANFANGSCHUFG OTTHIMMELUNDER DEUNDDIEERDEWA RWUESTUNDLEERU
NDESWARFINSTER AUFDERTIEFEUND DERGEISTGOTTES SCHWEBTEAUFDEM
WASSERUNDGOTTS PRACHESWERDELI CHTUNDESWARDLI CHTUNDGOTTSAHD
ASSDASLICHTGUT WAR
```

Am Anfang schuf Gott Himmel und Erde. Und die Erde war wüst und leer, und es war finster auf der Tiefe; und der Geist Gottes schwebte auf dem Wasser. Und Gott sprach: Es werde Licht! und es ward Licht. Und Gott sah, dass das Licht gut war.

Aus Genesis 1. Mose - Lutherbibel, 1. Kapitel - Die Schöpfung Vers 1-4

Kommentar:

Dass in diesem Kapitel die Herleitung einiger Formeln zu bewältigen ist, wird wahrscheinlich die meisten Schüler nicht sehr erfreuen. Hier sollte man aber versuchen ihnen klarzumachen, dass eine Chiffre, die lange Zeit als unbrechbar galt und von der man auch im vorhinein nicht vermutet, dass man sie (sogar per Hand) knacken kann, mit ein paar wenigen nicht allzu schwierig nachvollziehbaren Überlegungen völlig in die Knie zwingen kann.

Die Aufgaben sollten meiner Meinung nach in Gruppen gelöst werden, da es nicht ganz einfach ist, einen ganzen Geheimtext allein zu knacken. Außerdem wäre es hilfreich, Wörter bzw. Buchstaben mit Hilfe eines Programms zu zählen.

Anmerkung: Im Geheimtext des Beispiels aus Kapitel 2.3.2. (Kryptoanalyse der Vigenère- Chiffre) befindet sich ein „Fehler“: der 21. Buchstabe der 6. Spalte ist ein „Z“ und wird zu „y“ dechiffriert. Im Klartext steht deshalb das Wort „ihy“, was wahrscheinlich „ihr“ heißen müsste. Da das Beispiel aus einem Buch entnommen wurde, wurde dieser „Fehler“ aber beibehalten.

3. Das Problem der Schlüsselverteilung

3.1. Symmetrische Verschlüsselung

Alle bisher behandelten Chiffren waren symmetrische Verfahren, wo man zum Ver- und Entschlüsseln denselben Schlüssel benutzt. Das bedeutet aber immer, dass der Schlüssel zwischen den beiden Kommunikationspartnern ausgetauscht bzw. vereinbart werden muss. Doch kann das überhaupt auf sicherem Weg geschehen?

Ein Beispiel:
Eine Firma will einem Kunden vertrauliche Daten mitteilen, befürchtet aber, dass die Telefonverbindung abgehört wird. Deshalb wählt die Firma einen Schlüssel und chiffriert das Datenpaket mit DES. Der Kunde braucht nun aber den Schlüssel, um die Sendung zu dechiffrieren. Nun stellt sich aber wieder das Problem, wie die Firma dem Kunden den Schlüssel auf sicherem Wege mitteilen kann…

Der einzig sichere Weg wäre, den Schlüssel persönlich zu überbringen. Noch eine Möglichkeit, die aber schon weniger sicher ist, besteht darin, den Schlüssel mit einem Kurier oder per Post zu schicken. Früher wurde das in der Tat so gemacht, doch der große Nachteil daran ist, dass man immer schon eine Woche oder zumindest einige Tage, bevor man etwas Vertrauliches übermitteln wollte, den Schlüssel schicken musste.
Früher war das vielleicht noch machbar, doch heutzutage müssen so viele Daten möglichst schnell übermittelt werden. Durch die Vielzahl der Daten wird die Schlüsselverteilung zu einem großen logistischen Problem und auch der Zeitaufwand ist nicht mehr annehmbar.

Mit dem Problem der Schlüsselverteilung haben die Kryptographen schon immer gekämpft. Egal, wie sicher ein Chiffriersystem theoretisch ist, der Schlüsselaustausch ist immer die Schwachstelle.
Viele Kryptologen waren lange Zeit der Meinung, dieses Problem sei unlösbar, da der Schlüsselaustausch ein unvermeidbarer Teil der Verschlüsselung ist.
Doch Mitte der Siebzigerjahre wurde schließlich eine brillante Lösung entdeckt: Whitfield Diffie und Martin Hellman schlugen 1976 ein Verfahren vor, bei dem das Problem des Schlüsselaustausch umgangen werden kann.

Diffie- Hellman- Verfahren des Schlüsselaustauschs:

Bei diesem Verfahren muss der eigentliche Schlüssel gar nicht ausgetauscht werden. Die Grundlage für den Diffie- Hellman- Schlüsselaustausch sind sogenannte **Einweg- Funktionen**. Eine Einweg- Funktion ist nicht umkehrbar, d.h. sie ist leicht ausführbar, aber unmöglich oder sehr schwer wieder umzukehren.

Ein anschauliches Beispiel für eine Einweg- Funktion ist das Suchen einer Telefonnummer im Telefonbuch einer größeren Stadt: Kennt man den Namen lässt sich die dazugehörige Telefonnummer leicht finden. Sucht man jedoch umgekehrt einen Namen zu einer bekannten Telefonnummer, ist es um ein Vielfaches aufwändiger, diesen zu finden.

In der Modul- Arithmetik finden sich viele Einwegfunktionen. Das Verfahren für den Schlüsselaustausch von Diffie und Hellman beruht auf einer Einwegfunktion der Form $Y^x(\mathrm{mod}P)$. Kennt man den Wert von x, lässt sich leicht das Ergebnis der Funktion $Y^x(\mathrm{mod}P)$ berechnen, kennt man jedoch nur das Ergebnis, lässt sich kaum auf den Wert von X schließen.

Wollen nun zwei Kommunikationspartner, im folgenden Beispiel Alice und Bob genannt, einen geheimen Schlüssel austauschen, einigen sie sich erst einmal auf eine Funktion der Form $Y^x(\mathrm{mod}P)$, etwa Y=7 und P=11 (dabei müssen sie beachten, dass Y<P sein muss).
Sie haben sich also auf die Einweg- Funktion $7^x(\mathrm{mod}11)$ geeinigt, dies ist kein Geheimnis. Die Berechnung des Schlüssels erfolgt nun in 4 Schritten, wobei der eigentliche Schlüssel niemals ausgetauscht werden muss:

	Alice	Bob
1.Schritt:	Alice wählt eine geheime Zahl A, z.B. A=3.	Bob wählt eine geheime Zahl B, z.B. B=6.
2.Schritt:	Alice setzt A in die Einweg-Funktion ein und berechnet $\alpha=Y^A(\text{modP})$: $\alpha=7^3(\text{mod}11)=343(\text{mod}11)=2$.	Bob setzt B in die Einweg- Funktion ein und berechnet $\beta=Y^B(\text{modP})$: $\beta=7^6(\text{mod}11)=117649(\text{mod}11)=4$.
3.Schritt:	Alice schickt α=2 an Bob.	Bob schickt β=4 an Alice.
4.Schritt:	Alice berechnet den Schlüssel $k= \beta^A(\text{modP})$: $4^3(\text{mod}11)=64(\text{mod}11)=9$	Bob berechnet den Schlüssel $k= \alpha^B(\text{modP})$: $2^6(\text{mod}11)=64(\text{mod}11)=9$

Am Ende besitzen beide den Schlüssel k=9, obwohl dieser nie übermittelt werden musste. Sie erhalten auch sicher beide den gleichen Schlüssel, da:

$$\beta^A(\text{modP}) \overset{\beta=Y^B(\text{modP})}{=} Y^{B.A}(\text{modP}) = Y^{A.B}(\text{modP}) \overset{\alpha=Y^A(\text{modP})}{=} \alpha^B(\text{modP}).$$

Wenn jemand die Kommunikation von Alice und Bob abhört, erfährt er höchstens Y, P, α und β. A und B sind aber geheim, denn sie wurden nie ausgetauscht.
Der „Spion“ weiß nun, dass $Y^A(\text{modP})=\alpha$, also im vorigen Beispiel $7^A(\text{mod}11)=2$, außerdem weiß er, dass $Y^B(\text{modP})= \beta$, also $7^B(\text{mod}11)=4$. Da diese Funktionen Einweg- Funktionen sind, ist es (besonders bei großen Zahlen) sehr schwierig A oder B zu berechnen. Ohne die Zahlen A oder B kann aber der Schlüssel nicht berechnet werden!

Das Schlüsselaustausch- Problem wurde also dadurch umgangen, dass gerade genug Informationen ausgetauscht werden, damit Alice und Bob den Schlüssel berechnen können, aber zu wenig Informationen, dass damit irgendjemand sonst den Schlüssel berechnen könnte.

Das Diffie- Hellman- Verfahren war ein Durchbruch in der Geschichte der Kryptologie, doch das Verfahren war noch recht umständlich: Alice kann nämlich nicht spontan eine Nachricht an Bob schicken, denn sie muss erst auf eine Antwort von Bob warten, damit sie den Schlüssel berechnen kann.
Doch diese Idee brachte einen gewaltigen Sprung nach vorne und bewies endgültig, dass das Schlüsselverteilungsproblem überhaupt lösbar ist!

3.2. Asymmetrische Verschlüsselung

Die asymmetrische Verschlüsselung beruht auf einer Idee von Whitfield Diffie. Er hatte ein neues Verschlüsselungsverfahren entwickelt, wobei das Entschlüsseln nicht einfach die Umkehrung des Verschlüsselns ist (symmetrisches Verfahren), sondern bei der asymmetrischen Verschlüsselung sind Verschlüsselungs- und Entschlüsselungs- Schlüssel verschieden.
Diffie entwickelte zwar den Begriff der asymmetrischen Verschlüsselung, doch ein konkretes Beispiel dafür konnte er nicht vorweisen. Wenn aber die Kryptologen ein funktionierendes asymmetrisches Verschlüsselungsverfahren finden konnten, wäre dies eine Revolution in der Kryptologie.

Die asymmetrische Verschlüsselung wird auch als **Public- Key- Kryptographie** bezeichnet. Der Dechiffrierschlüssel bleibt geheim, er wird deshalb als **privater Schlüssel** bezeichnet. Der Chiffrierschlüssel wird veröffentlicht und steht allen zur Verfügung, deswegen heißt er **öffentlicher Schlüssel**.

Vorteile der asymmetrischen Verschlüsselungsverfahren

- Spontane Kommunikation ist möglich:
  Anders als bei symmetrischen Verfahren oder beim Diffie- Hellman- Verfahren müssen hier vorher keine Verabredungen über den Schlüssel getroffen werden.
- Problem des Schlüsselaustausch ist gelöst:
  Der private Schlüssel muss nicht ausgetauscht werden und der öffentliche Schlüssel muss nicht sicher übermittelt werden, jeder kann ihn erfahren.

- Man braucht wenige Schlüssel:
  Bei symmetrischen Verfahren benötigen je zwei Teilnehmer einen gemeinsamen Schlüssel, n Teilnehmer brauchen n.(n-1)/2 Schlüssel, d.h. die Anzahl der Schlüssel steigt quadratisch mit der Anzahl der Teilnehmer. Bei asymmetrischen Verfahren braucht jeder Teilnehmer nur zwei Schlüssel, einen privaten und einen öffentlichen. Der öffentliche Schlüssel kann von jedem anderen Teilnehmer verwendet werden. Die Anzahl der Schlüssel ist also nur doppelt so groß wie die Anzahl der Teilnehmer.
  z.B. brauchen 500 Teilnehmer in einem symmetrischen System 100 000 Schlüssel, wogegen in einem asymmetrischen System für 500 Teilnehmer nur 1000 Schlüssel benötigt werden, das ist nur 1% der Schlüssel im symmetrischen System.

3.3. Der RSA- Algorithmus

Um die Idee der asymmetrischen Verschlüsselung zu verwirklichen, braucht man einen Chiffrierschlüssel, mit dem man die Nachricht ver- aber nicht wieder entschlüsseln kann, also eine Einwegfunktion. Dazu muss es aber einen Dechiffrierschlüssel geben, um die Nachricht wieder zu entschlüsseln.
Gesucht wurde also nach einer speziellen Einwegfunktion (öffentlicher Schlüssel), die man mit einer besonderen Information (privater Schlüssel) wieder umkehren kann.
Nicht nur Diffie und Hellman begaben sich auf die Suche nach dieser Funktion, es begann ein Wettrennen um die Verwirklichung der asymmetrischen Verschlüsselung. Im Mai 1977 gewann ein Forscherteam, bestehend aus Ron Rivest, Adi Shamir und Leonard Adleman, dieses Rennen: Sie entwickelten den nach ihnen benannten RSA-Algorithmus.

Angenommen, Bob will Alice eine RSA- verschlüsselte Nachricht schicken:

3.3.1. Schlüsselerzeugung

Alice wählt zufällig zwei große Primzahlen p und q und berechnet das Produkt N=p.q. Außerdem berechnet sie (p-1).(q-1).

Danach wählt sie eine natürliche Zahl e, die zwischen 1 und (p-1).(q-1) liegt und zu (p-1).(q-1) teilerfremd ist, d.h. ggT(e, (p-1).(q-1))=1.
Schließlich berechnet sie die natürliche Zahl d, die wieder zwischen 1 und (p-1).(q-1) liegen muss, die d.e(mod(p-1).(q-1))=1 erfüllt.

Der **öffentliche Schlüssel**, den auch Bob verwenden kann, besteht aus dem Paar **(N,e)**, wobei N das Modul und e der Exponent genannt wird. **d** ist der **private Schlüssel**, den nur Alice kennt, dabei wurde d mittels p und q berechnet, deren Werte auch nur Alice kennt. Werden p und q groß genug gewählt, ist es praktisch unmöglich für einen Angreifer von N auf p und q zu schließen.

3.3.2. Verschlüsselung

Damit eine Nachricht verschlüsselt werden kann, muss sie zunächst in eine Zahl verwandelt werden. Das geschieht meist so, idem der Text mittels ASCCI- Code in eine binäre Zahl und diese wiederum in eine Dezimalzahl umgewandelt wird, man könnte aber auch alle Buchstaben in Zahlen umwandeln, indem man A=01, B=02, …, Z=26 setzt.
Der Klartext M sollte dann eine Zahl zwischen 1 und N-1 sein, falls M größer ist, wird die Zahl in Blöcke geteilt. M wird mit folgender Formel zum Geheimtext C verschlüsselt: $\mathbf{C=M^e(modN)}$.

Bob und jeder, der den öffentlichen Schlüssel (n,e) kennt, kann die Verschlüsselung durchführen.

3.3.3. Entschlüsselung

Zur Entschlüsselung wird der private Schlüssel d benötigt, man erhält den Klartext mit folgender Formel: $\mathbf{M=C^d(modN)}$.

Nur Alice kann den Geheimtext dechiffrieren, denn nur sie kennt den privaten Schlüssel d.

Ein Beispiel: (aus Simon Singh: Geheime Botschaften, Seite 436)

Alice wählt zwei Primzahlen p=17 und q=11 und berechnet N=p.q=187 und (p-1).(q-1)=160.
Als nächstes wählt sie den Exponenten e=7 (wobei e teilerfremd zu p und q ist und zwischen 1 und 160 liegt) und veröffentlicht N und e, d.h. Alice´s öffentlicher Schlüssel ist (187,7).
Danach berechnet sie ihren privaten Schlüssel d:
e.d (mod(p-1).(q-1))=1
7.d (mod160)=1
d=23, da 7.23(mod160)=161(mod160)=1

Bob will Alice einen symbolischen Kuss mit dem Buchstaben X schicken. In ASCCI wird X durch 1011000 dargestellt, was der Dezimalzahl 88 entspricht. Also M=88.
Bob verschlüsselt mit Alice´s öffentlichen Schlüssel (187,7) die Nachricht:
$C=88^7(\text{mod}187)$
88^7=40 867 559 636 992
40 867 559 636 992 :187=218 543 099 663 und 11 Rest
Also $C=88^7(\text{mod}187)=11$
Bob schickt den Geheimtext C=11 an Alice.

Alice entschlüsselt die Nachricht mit ihrem privaten Schlüssel d=23:
$M=C^d(\text{mod}187)$
$M=11^{23}(\text{mod}187)$=895 430 243 255 237 372 246 531(mod187)= 88= X in ASCCI

Aufgaben:

1. Verschlüssle den Klartext RSA mit dem öffentlichen Schlüssel (253,3), wobei A=01, B=02,… Z=26!

Lösung:
Der Klartext RSA wir zuerst in eine Zahl umgewandelt, R=18, S=19, A=01. Also M=181901.
Der Einfachheit halber verschlüsseln wir den Klartext blockweise:
$C=M^e(\text{mod}N)$

18^3(mod253)= 5832(mod253)= 13

19^3(mod253)= 6859(mod253)= 28

01^3(mod253)= 1(mod253)= 01

Also C=132801

2. Entschlüssle den Geheimtext 132801 blockweise mit p=11, q=23 und e=3, wobei A=01, B=02,… Z=26!

Lösung:

N=p.q=11.23=253

(p-1).(q-1)=10.22=220

d.e(mod(p-1).(q-1))=1

d.3(mod220)=1

d=147, da 147.3(mod220)= 441(mod220)=1

Mit dem privaten Schlüssel d kann der Geheimtext entschlüsselt werden:

$M=C^d$(modN)

13^{147}(mod253)= 18

28^{147}(mod253)= 19

01^{147}(mod253)= 01

Also M=181901, der Klartext lautet RSA.

Kommentar:

Weil der RSA- Algorithmus große Rechenkapazitäten benötigt, wird er oft nur dazu verwendet, um bei symmetrischen Verfahren, z.B. DES, den Schlüssel zu verschlüsseln und somit sicher zu übermitteln.

Das letzte Kapitel „Der RSA- Algorithmus“ soll nur einen Einblick in die moderne Kryptologie gewähren und verzichtet deshalb auf ausführlichere Behandlung. Wer jedoch dieses Thema oder allgemein die Public- Key- Kryptologie noch genauer im Unterricht behandeln will, dem empfehle ich Albrecht Beutelspacher: Kryptologie, 7. verbesserte Auflage, Seite 93 ff. und Simon Singh: Geheime Botschaften, 6. Auflage, Seite 329 ff zu lesen.

Literaturverzeichnis:

Bauer, Friedrich L.: Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie. 3., überarbeitete und erweiterte Auflage
Springer Verlag, Berlin 1995

Beutelspacher, Albrecht: Kryptologie, Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. 7., verbesserte Auflage
Vieweg- Verlag, Braunschweig 1987

Beutelspacher, Albrecht: Kryptografie in Theorie und Praxis
Vieweg- Verlag, Wiesbaden 2005

Beutelspacher, Albrecht: Moderne Verfahren der Kryptographie
Vieweg- Verlag, Braunschweig 1995

Büchter, Andreas: Mathematikaufgaben selbst entwickeln: Lernen fördern - Leistung überprüfen, 1. Auflage
Cornelsen Scriptor, Berlin 2005

Franke, H.W.: Die geheime Nachricht
Umschau, Frankfurt 1982

Lahmer, Margit: Kryptologie
Diplomarbeit am Institut für Mathematik der Universität Wien 2001

Leuders, Timo: Qualität im Mathematikunterricht der Sekundarstufe I und II
Cornelson Scriptor, Berlin 2001

Singh, Simon: Codes, Die Kunst der Verschlüsselung: Die Geschichte- Die Geheimnisse- Die Tricks
Carl Hanser Verlag, München, Wien 2002

Singh, Simon: Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, 6. Auflage
Dt. Taschenbuch-Verlag, München 2005

Internetquellen:

http://www.franzwest.at/gemeier/fraMit.htm
http://de.wikipedia.org/wiki/Palindrom
http://de.wikipedia.org/wiki/Kryptographie
http://de.wikipedia.org/wiki/Kryptologie
http://www.sicherheit-macht-schule.de/media/pdf/563.pdf
http://de.wikipedia.org/wiki/Pangramm
http://de.wikipedia.org/wiki/Isogramm
http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/1_Monoalph/Araber.html
http://martin-moeller.jimdo.com/krypto_-_freimaurerchiffre.php
http://www.gat-blankenburg.de/pages/fach/info/frei.htm
http://www.code-knacker.de/verschluesselung.htm
http://de.wikipedia.org/wiki/Mustersuche_(Kryptologie)
http://de.wikipedia.org/wiki/Buchstabenh%C3%A4ufigkeit
archiv.tu-chemnitz.de/pub/2002/0059/index.html
http://de.wikipedia.org/wiki/Mathematik
http://www.realschule-im-ghz.de/matheged.html
http://www.tinohempel.de/info/info/kryptografie/download/krypto.pdf
http://www.zahlenjagd.at/artikel97.html

Verwendete Programme im Internet:

Zur Häufigkeitsanalyse:
http://www.kas.bc.bw.schule.de/krypto/analyse.php
Zur Vigenère- Verschlüsselung:
http://www.lucius-hartmann.ch/diverse/kryptographie/vigenere.html

Marion Pilat

Lebenslauf

Persönliche Daten

Adresse	Brunnkirchner Hauptstraße 15, 3511 Krems- Brunnkirchen
Geburtsdatum, -ort	10.12.1984, Krems a.d. Donau
Familienstand	Ledig
Staatsbürgerschaft	Österreich

Ausbildung

seit 2003	Lehramtsstudium UF Mathematik und UF Biologie und Umweltkunde an der Universität Wien
2003	Matura mit ausgezeichnetem Erfolg
1995/96- 2002/03	Bundesrealgymnasium Ringstraße, Krems
1990/91-1994/95	Volksschule, Stein

Besondere Kenntnisse

Fremdsprachen	Englisch - Maturaniveau Französisch - Grundkenntnisse Spanisch - Grundkenntnisse
Sport	Ausbildung zur Snowboardbegleitlehrerin
Nachhilfe	Nachhilfeerfahrung im Fach Mathematik

Interessen

Sport	Schi, Snowboard, Kitesurfen, Karate, Capoeira
Sonstiges	Kochen, Backen, Reisen, Lesen, Jonglieren, Trommeln

Mautern, 15.12.2008

Abstract

In dieser Diplomarbeit wird das Thema Kryptologie für das Mathematik Wahlpflichtfach aufbereitet. Sie soll einen guten Einblick in die Kryptologie, von mono- und polyalphabetischer Verschlüsselung über Möglichkeiten, Verschlüsselungen zu knacken bis hin zu moderner Kryptologie, geben.
In den einzelnen Kapiteln wird meist zuerst kurz der geschichtliche Hintergrund behandelt, dann die Theorie möglichst verständlich und mit Beispielen erklärt und noch einige Übungsaufgaben samt Lösung vorgestellt.

In this diploma thesis the subject cryptology is prepared to be presented in the compulsory optional subject mathematics. It is supposed to provide a good insight in cryptology, from mono- and polyalphabetical encryption, via possibilities to crack encryptions, up to modern cryptology.
The individual chapters often start with some historical information, followed by a theory-part, explained understandingly with some examples, and several exercises with the corresponding solutions.