2 Kryptoanalyse der klassischen Verfahren

2.1 Klassifikation von Angriffen gegen Kryptosysteme

Die Erfolgsaussichten eines Angriffs gegen ein Kryptosystem hängen sehr stark davon ab, wie gut die Ausgangslage ist, in der sich der Gegner befindet. Prinzipiell sollte man die Fähigkeiten des Gegners genauso wenig unterschätzen wie die Unvorsichtigkeit der Anwender von Kryptosystemen. Bereits vor mehr als einem Jahrhundert postulierte Kerckhoffs, dass die Frage der Sicherheit keinesfalls von irgendwelchen obskuren Annahmen über den Wissensstand des Gegners abhängig gemacht werden darf.

Goldene Regel für Kryptosystem-Designer (auch „Kerckhoffs' Prinzip" genannt)
Unterschätze niemals den Kryptoanalytiker. Gehe insbesondere immer von der Annahme aus, dass dem Gegner das angewandte System bekannt ist.[*]

In der folgenden Liste sind eine Reihe von Angriffsszenarien mit zunehmender Gefährlichkeit aufgeführt. Auch wenn nicht alle Eventualitäten eines Angriffs vorhersehbar sind, so vermittelt diese Aufstellung doch eine gute Vorstellung davon, welchen unterschiedlichen Bedrohungen ein Kryptosystem im praktischen Einsatz ausgesetzt sein kann.

Angriff bei bekanntem Kryptotext (*ciphertext-only attack*)
Der Gegner fängt Kryptotexte ab und versucht, allein aus ihrer Kenntnis Rückschlüsse auf die zugehörigen Klartexte oder auf die benutzten Schlüssel zu ziehen.

Angriff bei bekanntem Klartext (*known-plaintext attack*)
Der Gegner ist im Besitz von einigen zusammengehörigen Klartext-Kryptotext-Paaren. Hierdurch wird erfahrungsgemäß die Entschlüsselung weiterer Kryptotexte oder die Bestimmung der benutzten Schlüssel wesentlich erleichtert.

Angriff bei frei wählbarem Klartext (*chosen-plaintext attack*)
Der Angriff des Gegners wird zusätzlich dadurch erleichtert, dass er in der Lage ist (oder zumindest eine Zeit lang war), sich zu Klartexten seiner Wahl die zugehörigen Kryptotexte zu besorgen. Kann hierbei die Wahl der Kryptotexte in Abhängigkeit von zuvor erhaltenen Verschlüsselungsergebnissen getroffen werden, so spricht man von einem **Angriff bei adaptiv wählbarem Klartext** (***adaptive chosen-plaintext attack***).

Angriff bei frei wählbarem Kryptotext (*chosen-ciphertext attack*)
Vor der Beobachtung des zu entschlüsselnden Kryptotextes konnte sich der Geg-

[*]Diese Annahme ergibt sich meist schon aus der Tatsache, dass die Prinzipien fast aller heute im Einsatz befindlichen Kryptosysteme allgemein bekannt sind.

ner zu Kryptotexten seiner Wahl die zugehörigen Klartexte besorgen, ohne dabei jedoch in den Besitz des Dechiffrierschlüssels zu kommen (**Mitternachtsattacke**). Das dabei erworbene Wissen steht ihm nun bei der Durchführung seines Angriffs zur Verfügung. Auch in diesem Fall können sich die Erfolgsaussichten des Gegners erhöhen, wenn ein **Angriff bei adaptiv wählbarem Kryptotext** (***adaptive chosen-ciphertext attack***) möglich ist, also der Kryptotext in Abhängigkeit von den zuvor erzielten Entschlüsselungsergebnissen wählbar ist.

Angriff bei frei (oder adaptiv) wählbarem Text (*chosen-text attack*)
Sowohl Klartexte als auch Kryptotexte sind frei (oder sogar adaptiv) wählbar.

Ohne Frage ist ein Kryptosystem, das bereits bei einem Angriff mit bekanntem Kryptotext Schwächen erkennen lässt, für den praktischen Einsatz vollkommen ungeeignet. Tatsächlich müssen aber an ein praxistaugliches Kryptosystem noch weit höhere Anforderungen gestellt werden. Denn häufig unterlaufen den Anwendern sogenannte **Chiffrierfehler**, die einen Gegner leicht in eine sehr viel günstigere Ausgangsposition versetzen als dies sonst der Fall wäre. So ermöglicht beispielsweise das Auftreten stereotyper Klartext-Formulierungen einen Angriff bei bekanntem Klartext, sofern der Gegner diese Formulierungen kennt oder auch nur errät. Begünstigt durch derartige Unvorsichtigkeiten, die im praktischen Einsatz nicht vollständig vermeidbar sind, können sich selbst winzige Konstruktionsschwächen eines Kryptosystems sehr schnell zu einer ernsthaften Bedrohung der damit verfolgten Sicherheitsinteressen auswachsen. Die Geschichte der Kryptographie belegt sehr eindrucksvoll, dass es häufig die Anwender eines Kryptosystems selbst sind, die – im unerschütterlichen Glauben an seine kryptographische Stärke – dem Gegner zum Erfolg verhelfen.

Zusammenfassend lässt sich also festhalten, dass die Gefährlichkeit von Angriffen, denen ein Kryptosystem im praktischen Einsatz ausgesetzt ist, kaum zu überschätzen ist. Andererseits kann selbst das beste Kryptosystem keinen Schutz vor einer unbefugten Dechiffrierung mehr bieten, wenn es dem Gegner etwa gelingt, in den Besitz des geheimen Schlüssels zu kommen – sei es aus Unachtsamkeit der Anwender oder infolge einer Gewaltandrohung des Gegners (**kompromittierte Schlüssel**).

2.2 Kryptoanalyse von einfachen Substitutionschiffren

Manche der bisher betrachteten Chiffrierverfahren verwenden einen so kleinen Schlüsselraum, dass ohne großen Aufwand eine vollständige Schlüsselsuche ausgeführt werden kann.

Beispiel 51 (vollständige Schlüsselsuche) *Es sei bekannt, dass das Kryptotextstück $y = \mathsf{SAXP}$ mit einer additiven Chiffre erzeugt wurde ($K = A = B = A_{lat}$). Entschlüsseln wir y probeweise mit allen möglichen Schlüsselwerten, so erhalten wir folgende Zeichenketten.*

k	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
$D(k,y)$	RZWO	QYVN	PXUM	OWTL	NVSK	MURJ	LTQI	KSPH	JROG	IQNF	HPME	GOLD

N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
FNKC	EMJB	DLIA	CKHZ	BJGY	AIFX	ZHEW	YGDV	XFCU	WEBT	VDAS	UCZR	TBYQ

Unter diesen springen vor allem die beiden Klartextkandidaten $x =$ GOLD (Schlüsselwert $k =$ M) und $x =$ WEBT ($k =$ W) ins Auge.

Ist $s = \|K\|$ die Größe des Schlüsselraums, so kann der Gegner bei bekanntem Kryptotext y die Suche nach dem zugehörigen Klartext x auf eine Menge von maximal s Texten $x_1, \ldots, x_s$ beschränken. Daneben hat der Gegner ein gewisses *a priori* Wissen über den Klartext, wie zum Beispiel dass er in deutscher Sprache verfasst ist, das es ihm gestattet, einen Großteil der Texte x_i auszuschließen. Ferner erscheinen aufgrund dieses Hintergrundwissens manche der übrig gebliebenen Klartextkandidaten plausibler als andere (sofern nicht nur ein einziger übrig bleibt). Mit jedem Text x_i, der nicht als Klartext in Frage kommt, kann auch mindestens ein Schlüssel ausgeschlossen werden. Sind noch mehrere Schlüsselwerte möglich, so kann weiteres Kryptotextmaterial Klarheit bringen. Manchmal hilft aber auch eine Inspektion der verbliebenen Schlüsselwerte weiter, etwa wenn der Schlüssel nicht rein zufällig erzeugt wurde, sondern aus einem einprägsamen Schlüsselwort ableitbar ist.

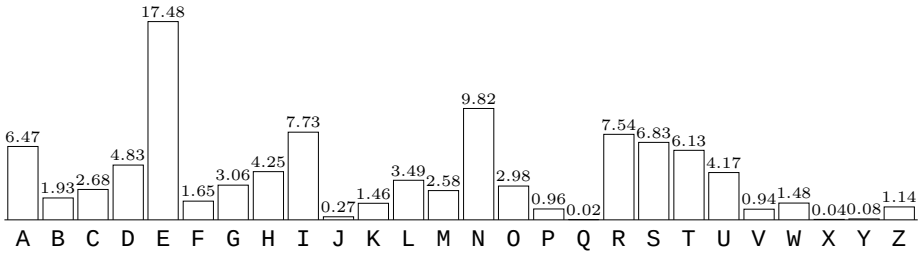

Abbildung 1 Häufigkeitsverteilung von Einzelbuchstaben im Deutschen (in %).

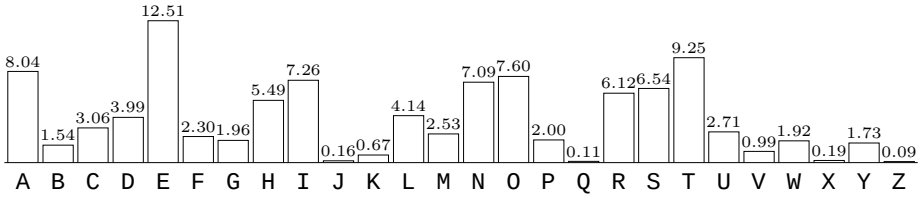

Abbildung 2 Häufigkeitsverteilung von Einzelbuchstaben im Englischen (in %).

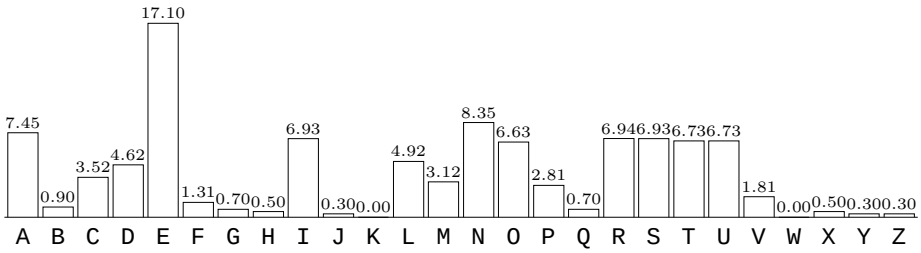

Abbildung 3 Häufigkeitsverteilung von Einzelbuchstaben im Französischen (in %).

Meist kennt der Gegner zumindest die Sprache, in der der gesuchte Klartext abgefasst ist. Mit zunehmender Länge gleichen sich die Häufigkeitsverteilungen der Buchstaben in natürlichsprachigen Texten einer „Grenzverteilung“ an, die in erster Linie von der benutzten Sprache und nur in geringem Umfang von der Art des Textes abhängt. Diese Verteilungen weisen typischerweise eine sehr starke Ungleichmäßigkeit auf, was darauf zurückzuführen ist, dass in natürlichen Sprachen relativ viel Redundanz enthalten ist. Die Abbildungen 1, 2 und 3, zeigen typische Verteilungen von Einzelbuchstaben in der deutschen, englischen und französischen Sprache (ohne Berücksichtigung von Interpunktions- und Leerzeichen). Ein typischer deutscher Text besteht demnach zu 62% aus den sieben häufigsten Zeichen E, N, I, R, S, A, T (das sind nicht einmal 27% der Klartextzeichen).

Bei additiven Chiffren reicht es oftmals, den häufigsten Buchstaben im Kryptotext zu bestimmen, und davon den häufigsten Buchstaben der Klartextsprache zu subtrahieren, um den Schlüssel k zu erhalten. Bei affinen Chiffren müssen gewöhnlich nur die beiden häufigsten Buchstaben bestimmt werden; dadurch erhält man zwei Verschlüsselungsgleichungen. Dieses Gleichungssystem muss gelöst werden, und man erhält das gesuchte Schlüsselpaar.

Beispiel 52 (Analyse einer affinen Chiffre mittels Buchstabenhäufigkeiten) *Es sei bekannt, dass sich hinter dem Kryptotext*

```
laoea ehoap hwvae ixobg jcbho thlob lokhe ixope vbcix ockix
qoppo boapo mohqc euogk opeho jhkpl eappj seobe ixoap opmcu
```

ein deutscher Klartext verbirgt, der mit einer additiven Chiffre verschlüsselt wurde. Berechnen wir für jedes Chiffrezeichen y die (absolute) Häufigkeit $H(y)$ seines Auftretens,

y	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
$H(y)$	7	6	5	0	10	0	2	8	5	3	4	4	2	0	19	11	2	0	1	1	2	2	1	5	0	0

so liegt die Vermutung nahe, dass das am häufigsten vorkommende Chiffrezeichen P für das Klartextzeichen E und das am zweithäufigsten vorkommende O für N steht. Unter dieser Annahme kann der gesuchte Schlüssel $k = (b, c)$ als Lösung der beiden Gleichungen

$$\begin{aligned} b \cdot \mathsf{E} + c &= \mathsf{O} \\ b \cdot \mathsf{N} + c &= \mathsf{P} \end{aligned}$$

bestimmt werden. Subtrahieren wir nämlich die erste von der zweiten Gleichung, so erhalten wir die Kongruenz $9 \cdot b \equiv_{26} 1$, woraus sich $b = 3$ und damit $c = 2$ ergibt. Tatsächlich weist der Schlüssel $k = (3, 2)$ nicht nur für die beiden Paare (E, O) und (N, P), sondern auch für alle übrigen Paare (x, y) eine gute Übereinstimmung zwischen der Häufigkeit $H(y)$, mit der $y = E(k, x)$ im Kryptotext vorkommt, und der erwarteten Häufigkeit $E(x)$ auf, mit der x in einem typischen deutschen Text der Länge 100 vorkommt (die Tabelle zeigt die Werte von $E(x)$ gerundet):

x	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
$E(x)$	6	2	3	5	17	2	3	4	8	0	1	3	3	10	3	1	0	8	7	6	4	1	1	0	0	1
$H(y)$	5	0	5	4	19	0	2	5	7	0	2	3	2	11	1	2	0	6	10	8	4	0	2	1	1	0
y	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

Durch eine Häufigkeitsanalyse können insbesondere einfache Substitutionen g leicht gebrochen werden, sofern die einzelnen Buchstaben a in der benutzten Klartextsprache mit voneinander differierenden Häufigkeiten $p(a)$ auftreten (vergleiche Tabelle 1). Selbst wenn, was insbesondere bei kurzen Texten zu erwarten ist, die tatsächliche Häufigkeitsverteilung nur in etwa der vom Gegner angenommenen Verteilung entspricht, reduziert sich dadurch die Zahl der in Frage kommenden einfachen Substitutionen ganz erheblich. Berechnet man die relativen Häufigkeiten h der Kryptotextbuchstaben im Kryptotext, so gilt $p(a) \approx h(g(a))$ (vorausgesetzt der Kryptotext ist genügend lang). Für die Schilderung einer nach dieser Methode durchgeführten Kryptoanalse sei auf die Erzählung „Der Goldkäfer“ von Edgar Allan Poe verwiesen.

Tabelle 1 Einteilung von Buchstaben in Cliquen mit vergleichbaren Häufi gkeitswerten.

	Deutsch	Englisch	Französisch
sehr häufi g	E	E	E
häufi g	N | I R S | A T	T | A O I N | S R H	N | A R S I T U
durchschnittlich	D H U | L G O | C M	L D | C U M F	L D | C M P
selten	B F W K Z | P V	P G W Y B | V K	V | F B G Q H X
sehr selten	J Y X Q	X J Q Z	J Y Z K W

2.3 Kryptoanalyse von Blocktranspositionen

Mit Hilfe von Bigrammhäufigkeiten, die manchmal auch als Kontakthäufigkeiten bezeichnet werden, lassen sich Blocktranspositionen sehr leicht brechen, sofern genügend Kryptotext vorliegt. Ist die Blocklänge l bekannt, so trägt man hierzu den Kryptotext zeilenweise in eine Matrix $S = (s_{ij})$ mit l Spalten $S_1, \ldots, S_l$ ein. Da jede Zeile dieser Matrix aus dem zugehörigen Klartextblock mit derselben Permutation π erzeugt wurde, müssen die Spalten S_j jetzt nur noch in die „richtige“ Reihenfolge gebracht werden, um den gesuchten Klartext zu erhalten. Der Nachfolger S_k von S_j (bzw. der Vorgänger S_j von S_k) kann sehr gut anhand der Werte von $\hat{p}(S_j, S_k) = \sum_i p(s_{ij}, s_{ik})$ bestimmt werden.

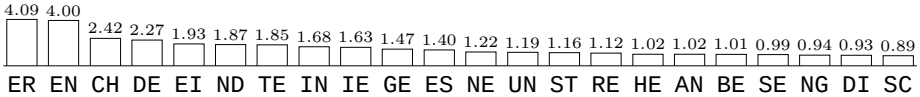

Abbildung 4 Die häufi gsten Bigramme im Deutschen (Angaben in %).

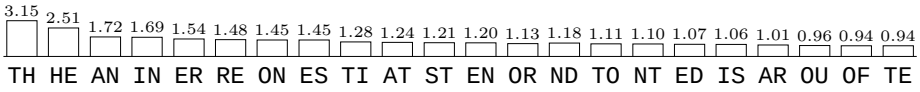

Abbildung 5 Die häufi gsten Bigramme im Englischen (in %; nach O.P. Meaker, 1939).

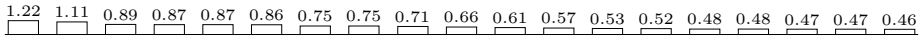

Abbildung 6 Die häufi gsten Trigramme im Deutschen (in %).

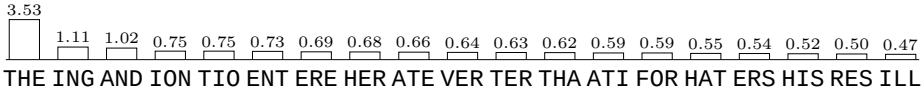

Abbildung 7 Die häufi gsten Trigramme im Englischen (in %).

Beispiel 53 (Häufigkeitsanalyse von Bigrammen) *Für den mit einer Blocktransposition (mit vermuteter Blocklänge 5) erzeugten Kryptotext*

IHEHR BWEAN RNEII NRKEU ELNZK RXTAE VLOTR ENGIE

erhalten wir eine Matrix S mit den folgenden fünf Spalten.

S_1	S_2	S_3	S_4	S_5
I	H	E	H	R
B	W	E	A	N
R	N	E	I	I
N	R	K	E	U
E	L	N	Z	K
R	X	T	A	E
V	L	O	T	R
E	N	G	I	E

Um die richtige Vorgänger- oder Nachfolgerspalte von S_1 zu finden, bestimmen wir für jede potentielle Spalte S_j, $j = 2, \ldots, 5$, wieviele der Bigramme $s_{ij}s_{i1}$ (bzw. $s_{i1}s_{ij}$) zu den 20 häufigsten (aus Abbildung 4) gehören.

				↓		↓		
S_2	S_3	S_4	S_5	S_1	S_2	S_3	S_4	S_5
H	**E**	H	R	**I**	H	**E**	H	R
W	E	A	N	**B**	W	**E**	A	N
N	**E**	I	I	**R**	N	**E**	I	I
R	K	**E**	**U**	**N**	R	K	**E**	U
L	**N**	Z	K	**E**	L	**N**	Z	K
X	T	A	**E**	**R**	X	T	A	**E**
L	O	T	R	V	L	O	T	R
N	**G**	**I**	E	**E**	**N**	G	**I**	E

Da die beiden Spaltenpaare (S_3, S_1) und (S_1, S_3) jeweils vier häufige Bigramme bilden, können wir annehmen, dass im Klartext S_1 auf S_3 oder S_3 auf S_1 folgen muss. Entscheiden wir uns für die zweite Möglichkeit, so sollten wir als nächstes die Spaltenpaare (S_j, S_1) und (S_3, S_j), $j = 2, 4, 5$ betrachten.

				↓				↓
S_2	S_4	S_5	S_1	S_3	S_2	S_4	S_5	
H	H	R	I	**E**	H	H	**R**	
W	A	N	B	**E**	W	A	**N**	
N	I	I	R	**E**	**N**	**I**	**I**	
R	**E**	**U**	**N**	K	R	E	U	
L	Z	K	E	N	L	Z	K	
X	A	**E**	**R**	**T**	X	A	**E**	
L	T	R	V	O	L	T	R	
N	**I**	E	**E**	**G**	N	I	**E**	

Aufgrund des hohen Wertes von $\hat{p}(S_3, S_5)$ können wir annehmen, dass auf S_3 die Spalte S_5 folgt. Im nächsten Schritt erhalten wir daher die folgende Tabelle.

	↓	↓		↓	↓	
S_2	S_4	S_1	S_3	S_5	S_2	S_4
H	H	I	E	R	H	H
W	A	B	E	N	W	A
N	I	R	E	**I**	**N**	I
R	**E**	**N**	K	U	R	E
L	Z	E	N	K	L	Z
X	A	R	T	E	X	A
L	T	V	O	R	L	T
N	**I**	**E**	G	**E**	**N**	**I**

Diese lässt die Spaltenanordnung S_4, S_1, S_3, S_5, S_2 vermuten, welche tatsächlich auf den gesuchten Klartext führt:

S_4	S_1	S_3	S_5	S_2
H	I	E	R	H
A	B	E	N	W
I	R	E	I	N
E	N	K	U	R
Z	E	N	K	L
A	R	T	E	X
T	V	O	R	L
I	E	G	E	N

2.4 Kryptoanalyse von polygraphischen Chiffren

Blocksysteme mit kleinem k (beispielsweise bigraphische Systeme) lassen sich ähnlich wie einfache Substitutionen durch Häufigkeitsanalysen brechen. Wird bei Hill-Chiffren k sehr groß gewählt, so ist eine solche statistische Analyse nicht mehr möglich. Das Hill-System kann dann zwar einem Kryptotextangriff widerstehen, jedoch kaum einem Angriff mit bekanntem Klartext und schon gar nicht einem Angriff mit gewähltem Klartext.

Angriff mit gewähltem Klartext O. B. d. A. sei $A = \{0, 1, \ldots, m-1\}$. Bei einem GK-Angriff verschafft sich der Gegner den Kryptotext zu $100\ldots0$, $010\ldots0$, …,

$0 \ldots 001 \in A^l$:

$$\begin{aligned} g(100\ldots0) &= k_{1\,1}\, k_{1\,2} \ldots k_{1\,l} \\ g(010\ldots0) &= k_{2\,1}\, k_{2\,2} \ldots k_{2\,l} \\ &\vdots \\ g(0\ldots001) &= k_{l\,1}\, k_{l\,2} \ldots k_{l\,l} \end{aligned}$$

und erhält damit die Schlüsselmatrix k.

BK-Angriff (bekannter Klartext). Sind bei einem BK-Angriff ausreichend geeignete Klartext-Kryptotextpaare bekannt, so kann das Hill-System folgendermaßen gebrochen werden: Sind x_i, y_i ($i = 1, \ldots, \mu$) Paare mit $x_i k = y_i$ und gilt $\mathrm{ggT}(\det X, m) = 1$ für eine aus l Blöcken x_i, $i \in I$, als Zeilen gebildete Matrix X, so lässt sich die Schlüsselmatrix k zu $k = YX^{-1}$ bestimmen (Y ist die aus den Blöcken y_i, $i \in I$, gebildete Matrix).

2.5 Kryptoanalyse von polyalphabetischen Chiffren

Die Vigenère-Chiffre galt bis ins 19. Jahrhundert als sicher. Da der Schlüsselstrom bei der Vigenère-Chiffre periodisch ist, lassen sie sich mit statistischen Methoden ebenfalls leicht brechen, insbesondere wenn der Kryptotext im Verhältnis zur Periode d (Länge des Schlüsselwortes) genügend lang ist.

Bestimmung der Schlüsselwortlänge

Es gibt mehrere Methoden, eine Vigenère-Chiffre zu brechen, sobald die Länge des Schlüsselwortes bekannt ist. So kann man beispielsweise den Kryptotext zeilenweise in eine d-spaltige Matrix schreiben. Verfahrensbedingt wurden dann die einzelnen Spalten $y_1, \ldots, y_d$ durch eine monoalphabetische Substitution (genauer: durch eine Verschiebechiffre) verschlüsselt. Sie können daher einzeln wie eine additive Chiffre durch eine Häufigkeitsanalyse gebrochen werden. Hierbei liefert jede Spalte y_i einen Buchstaben k_i des Schlüsselwortes der Vigenère-Chiffre.

Zur Bestimmung der Schlüsselwortlänge betrachten wir zwei Vorgehensweisen: den Kasiski-Test und die Koinzidenzindex-Untersuchung.

Der Kasiski-Test. Die früheste generelle Methode zur Bestimmung der Periode bei der Vigenère-Chiffre stammt von Friedrich W. Kasiski (1860). Kommt ein Wort an zwei verschiedenen Stellen im Kryptotext vor, so kann es sein, dass die gleiche Klartextsequenz zweimal auf die gleiche Weise, d. h. mit der gleichen Schlüsselsequenz, verschlüsselt wurde. In diesem Fall ist die Entfernung δ der beiden Vorkommen ein Vielfaches der Periode d. Werden mehrere Paare mit verschiedenen Entfernungen δ_i gefunden, so liegt die Vermutung nahe, dass d gemeinsamer Teiler aller (oder zumindest vieler) δ_i ist, was die Anzahl der noch in Frage kommenden Werte für d stark einschränkt.

Beispiel 54 (Kasiski-Test)

	DERERSTEUNDLETZTEVERS...	*(Klartext x)*
+	KASKASKASKASKASKASKAS...	*(Schlüsselstrom $\hat{k}$)*
	NEJORKDEMXDDOTRDENORK...	*(Kryptotext y)*

Dass die Textstücke ORK*, bzw.* DE *im Kryptotext in den Entfernungen $\delta_1 = 15$ und $\delta_2 = 9$ vorkommen, führt auf die richtige Vermutung, dass die Periode $d = \mathrm{ggT}(9, 15) = 3$ ist.*

Koinzidenzindex-Untersuchungen. Zur Bestimmung der Periode d gibt es neben heuristischen Methoden auch folgenden statistischen Ansatz, der erstmals von William Frederick Friedman im Jahr 1920 beschrieben wurde. Er basiert auf der Beobachtung, dass eine längere Periode eine zunehmende *Glättung* der Buchstabenhäufigkeiten im Kryptotext bewirkt.

Definition 55 (Koinzidenzindex)

Der ***Koinzidenzindex*** (engl. ***i**ndex of **c**oincidence*) eines Textes y der Länge n über dem Alphabet $\mathcal{B}$ ist definiert als

$$IC(y) = \frac{1}{n \cdot (n-1)} \cdot \sum_{a \in \mathcal{B}} H(a) \cdot (H(a) - 1).$$

Hierbei ist $H(a)$ die absolute Häufigkeit des Buchstabens a im Text y.

$IC(y)$ gibt also die Wahrscheinlichkeit an, mit der man im Text y an zwei zufällig gewählten Positionen den gleichen Buchstaben vorfindet. Er ist umso größer, je ungleichmäßiger die Häufigkeiten $H(a)$ sind (siehe unten).

Um die Periode d einer Vigenère-Chiffre zu bestimmen, schreibt man den Kryptotext y für $d = 1, 2, 3, \ldots$ in eine Matrix mit d Spalten und berechnet für jede Spalte y_i den Koinzidenzindex. Für genügend lange Kryptotexte ist dasjenige d, welches das maximale arithmetische Mittel der Spaltenindizes liefert mit hoher Wahrscheinlichkeit die gesuchte Periode. Enthält eine Spalte nämlich nur Kryptozeichen, die alle mit demselben Schlüsselbuchstaben k erzeugt wurden, so stimmt der Koinzidenzindex dieser Spalte mit dem Koinzidenzindex des zugehörigen Klartextes überein, nimmt also einen relativ großen Wert an. Wurden dagegen die Kryptozeichen einer Spalte mit unterschiedlichen Schlüsselbuchstaben generiert, so wird hierdurch eine Glättung der Häufigkeitsverteilung bewirkt, weshalb der Spaltenindex kleiner ausfällt.

Ist die Einzelbuchstabenverteilung $p : A \to [0, 1]$ der Klartextsprache bekannt, so kann der Suchraum für den Wert der Periode d erheblich eingeschränkt werden. Hierzu berechnet man den erwarteten Koinzidenzindex $\mathrm{E}(IC)$ des Kryptotextes in Abhängigkeit von d. Ist $d = 1$, so ist $IC(y) = IC(x)$. Bei längeren Texten können wir von den gegenseitigen Abhängigkeiten der Zeichen im Text absehen und erhalten

$$\mathrm{E}(IC) = \sum_{a \in A} p(a)^2.$$

als Erwartungswert für den Koinzidenzindex. Dieser Wert wird auch als Koinzidenzindex der zugrunde liegenden Sprache bezeichnet.

Definition 56 (**Koinzidenzindex einer Sprache**)

Der ***Koinzidenzindex*** IC_L ***einer Sprache*** mit Buchstabenverteilung $p : A \to [0,1]$ ist definiert als

$$IC_L = \sum_{a \in A} p(a)^2.$$

IC_L ist zudem ein Maß für die Rauheit der Verteilung p:

Definition 57 (**Rauheitsgrad; Measure of Roughness**)

Der ***Rauheitsgrad*** MR_L einer Sprache L mit Einzelbuchstabenverteilung p ist

$$MR_L = \sum_{a \in A} (p(a) - 1/m)^2 = \sum_{a \in A} p(a)^2 - 1/m = IC_L - 1/m,$$

wobei $m = \|A\|$ ist.

Beispiel 58 *Für die englische Sprache (*$m = 26$*) gilt beispielsweise* $IC_{\text{Englisch}} \approx 0{,}0687$ *und* $MR_{\text{Englisch}} \approx 0{,}0302$.

Übersteigt dagegen d die Klartextlänge n, so ist der Kryptotext bei zufälliger Wahl des Schlüsselswortes ebenfalls rein zufällig, was auf einen erwarteten Koinzidenzindex von

$$\mathrm{E}(IC) = \sum_{a \in A} \|A\|^{-2} = \|A\|^{-1}$$

führt. Allgemein gilt

$$\mathrm{E}(IC) = \frac{n-d}{d \cdot (n-1)} \cdot IC_L + \frac{n \cdot (d-1)}{d \cdot (n-1)} \cdot \|A\|^{-1},$$

da von den $\binom{n}{2} = n(n-1)/2$ möglichen Positionspaaren ungefähr $d \cdot \binom{n/d}{2} = n(n-d)/2d$ Paare nur eine Spalte und $\binom{d}{2}(n/d)^2 = n^2(d-1)/2d$ Paare zwei unterschiedliche Spalten betreffen.

Untenstehende Tabelle gibt den Erwartungswert $\mathrm{E}(IC)$ des Koinzidenzindexes für Kryptotexte der Länge $n = 100$ in Abhängigkeit von der Periodenlänge d einer Vigenère-Chiffre wieder (in Promille; Klartext ist ein zufällig gewählter Text der englischen Sprache).

d	1	2	3	4	5	6	8	10	∞
$\mathrm{E}(IC)$	69	54	48	46	44	43	42	41	39

Beispiel 59 *Berechnet sich der Koinzidenzindex eines Vigenère-Kryptotextes der Länge* 100 *zu* 0,045*, so liegt die Vermutung nahe, dass das verwendete Schlüsselwort die Länge vier oder fünf hat, falls* y *aus einem Klartext der englischen Sprache erzeugt wurde.*

Der Koinzidenzindex kann auch Hinweise dafür liefern, mit welchem Kryptoverfahren ein vorliegender Kryptotext erzeugt wurde. Bei Transpositionschiffren sowie bei einfachen Substitutionen bleibt nämlich der Koinzidenzindex im Gegensatz zu polyalphabetischen und polygraphischen Verfahren erhalten. Erstere lassen sich von letzteren zudem dadurch unterscheiden, dass bei ihnen sogar die Buchstabenhäufigkeiten unverändert bleiben.

Zur Bestimmung des Schlüsselwortes bei bekannter Periode d kann auch wie folgt vorgegangen werden. Man schreibt den Kryptotext y in Spalten y_i auf und berechnet für $a \in A$ und $i = 1, \ldots, d$ die relativen Häufigkeiten $h_i(a)$ von a in y_i. Da y_i aus dem Klartext durch Addition von k_i entstanden ist, kommt die Verteilung

$$h_i(a+k), a \in A$$

für $k = k_i$ der Klartextverteilung $p(a), a \in A$ näher als für $k \neq k_i$. Da

$$\alpha_i(k) := \sum_{a \in A} p(a) h_i(a+k)$$

ein Maß für die Ähnlichkeit der beiden Verteilungen $p(a)$ und $h_i(a+k)$ ist (siehe Übungen), wird der Wert von $\alpha_i(k)$ wahrscheinlich für $k = k_i$ maximal werden.

Beispiel 60 *Der folgende Kryptotext y*

```
HUDS KUAE ZGXR AVTF PGWS WGWS ZHTP PBIL LRTZ PZHW
LOIJ VFIC VBTH LUGI LGPR KHWM YHTI UAXR BHTW UCGX
OSPW AOCH IMCS YHWQ HWCF YOCG OGTZ LBIL SWBF LOHX
ZWSI ZVDS ATGS THWI SSUX LMTS MHWI KSPX OGWI HRPF
LSAM USUV VAIL LHGI LHWV VIVL AVTW OCIJ PTIC MSTX
VII
```

der Länge 203 *wurde von einer Vigenère-Chiffre mit Schlüssellänge $d = 4$ aus englischem Klartext erzeugt. Schreiben wir den Kryptotext in vier Spalten $y_1, \ldots, y_4$ der Länge $|y_1| = |y_2| = |y_3| = 51$ und $|y_4| = 50$, so ergeben sich folgende Werte für $\alpha_i(k)$ (in Promille):*

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$\alpha_1(k)$	36	31	31	45	38	26	42	**73**	44	26	36	47	30
$\alpha_2(k)$	44	41	40	51	41	31	37	43	34	28	36	26	28
$\alpha_3(k)$	47	41	48	37	49	40	35	30	48	32	25	42	31
$\alpha_4(k)$	38	40	27	41	**65**	47	28	34	39	33	35	36	30

k	13	14	15	16	17	18	19	20	21	22	23	24	25
$\alpha_3(k)$	32	36	29	28	39	48	42	42	39	42	42	35	31
$\alpha_1(k)$	43	**68**	45	35	27	42	43	40	35	30	24	31	45
$\alpha_2(k)$	26	43	**76**	37	31	39	45	35	34	37	26	30	25
$\alpha_3(k)$	30	48	44	35	42	47	38	39	34	27	38	36	37

Da $\alpha_1(k)$ für $k = 7 =$ H, $\alpha_2(k)$ für $k = 14 =$ O, $\alpha_3(k)$ für $k = 15 =$ P und $\alpha_4(k)$ für $k = 4 =$ E einen Maximalwert annimmt, lautet das Schlüsselwort HOPE. Damit ergibt sich folgender Klartext

```
A GOOD GLASS IN THE BISHOPS HOSTEL IN THE DEVILS
SEAT FORTYONE DEGREES AND THIRTEEN MINUTES NORTH
EAST AND BY NORTH MAIN BRANCH SEVENTH LIMB EAST
SIDE SHOOT FROM THE LEFT EYE OF THE DEATHS HEAD
A BEE LINE FROM THE TREE THROUGH THE SHOT FIFTY
FEET OUT
```

Zur Bestimmung des Schlüsselwortes kann man auch die Methode des *gegenseitigen Koinzidenzindexes* verwenden. Dabei ist die verwendete Klartextsprache (und somit deren Häufigkeitsverteilung) irrelevant, da die Spalten – wie der Name schon sagt – gegenseitig in Relation gesetzt werden. Aber zuerst die Definition.

Definition 61 (**Gegenseitiger Koinzidenzindex**)

Der ***gegenseitge Koinzidenzindex*** von zwei Texten y und y' mit den Längen n und n' über dem Alphabet $\mathcal{B}$ ist definiert als

$$IC(y, y') = \frac{1}{n \cdot n'} \cdot \sum_{a \in \mathcal{B}} H(a) \cdot H'(a).$$

Hierbei ist $H(a)$ bzw. $H'(a)$ die absolute Häufigkeit des Buchstabens a im Text y bzw. y'.

$IC(y, y')$ ist also die Wahrscheinlichkeit, dass bei zufälliger Wahl einer Position in y und einer Position in y' der gleiche Buchstabe vorgefunden wird. $IC(y, y')$ ist umso größer, je besser die Häufigkeitsverteilung von y und y' (d. h. H und H') übereinstimmen.

Ist nun y ein Kryptotext, der mit einem Schlüsselwort bekannter Länge d erzeugt wurde, und sind y_i, $i = 1, \ldots, d$ die zugehörigen Spalten, so gibt der gegenseitige Koinzidenzindex der Spalten y_i und $y_j + \delta$ (für $1 \leq i < j \leq d$) die Wahrscheinlichkeit an, dass man bei zufälliger Wahl einer Position in y_i und in $y_j + \delta$ denselben Buchstaben vorfindet, wobei δ eine Verschiebung von Spalte y_j relativ zur Spalte y_i ist (mit $0 \leq \delta \leq 25$). Mit großer Wahrscheinlichkeit nimmt also $IC(y_i, y_j + \delta)$ für $\delta = \delta_{ij} = k_j - k_i$ einen relativ großen Wert an, während für $\delta \neq \delta_{ij}$ mit kleinen Werten zu rechnen ist.

Beispiel 62 *Betrachten wir den Kryptotext aus vorigem Beispiel, so ergeben sich für $IC(y_i, y_j + \delta)$ die folgenden Werte (in Promille):*

δ	0	1	2	3	4	5	6	7	8	9	10	11	12
$IC(y_1, y_2 + \delta)$	40	31	25	38	25	21	46	**74**	50	33	31	44	43
$IC(y_1, y_3 + \delta)$	26	47	25	21	47	32	18	49	**91**	42	27	51	45
$IC(y_1, y_4 + \delta)$	38	40	29	31	35	24	32	58	42	32	44	50	43
$IC(y_2, y_3 + \delta)$	50	**85**	49	21	28	35	24	34	46	25	24	27	59
$IC(y_2, y_4 + \delta)$	46	53	40	37	51	42	29	23	24	32	40	55	38
$IC(y_3, y_4 + \delta)$	49	36	38	60	36	25	34	19	29	42	41	33	54

δ	13	14	15	16	17	18	19	20	21	22	23	24	25
$IC(y_1, y_2 + \delta)$	34	31	28	24	31	44	45	37	48	64	44	25	31
$IC(y_1, y_3 + \delta)$	31	29	32	23	29	27	39	45	46	39	58	44	24
$IC(y_1, y_4 + \delta)$	39	31	20	34	36	30	40	45	24	42	**78**	47	22
$IC(y_2, y_3 + \delta)$	50	50	53	51	24	22	26	43	36	35	32	24	34
$IC(y_2, y_4 + \delta)$	31	32	45	**67**	49	25	27	29	29	34	37	38	35
$IC(y_3, y_4 + \delta)$	27	36	**78**	47	25	29	33	27	28	47	32	27	54

Also ist (mit großer Wahrscheinlichkeit)

$$\delta_{1\,2} = 7,\ \delta_{1\,3} = 8,\ \delta_{1\,4} = 23,\ \delta_{2\,3} = 1,\ \delta_{2\,4} = 16,\ \delta_{3\,4} = 15.$$

Wir können nun alle Spalten relativ zur ersten Spalte so verschieben, dass der ganze Text eine einheitliche Verschiebung δ hat, also die zweite Spalte um -7, die dritte um -8 und die vierte um -23. Für die Bestimmung von δ, muss man nur den häufigsten Buchstaben in dem auf diese Weise erzeugten Text bestimmen. Dieser ist L *($16,3\%$). Also ist $\delta =$ L $-$ E $=$ H $= 7$ und das Schlüsselwort lautet* HOPE *(H$+7=$O, H$+8=$P, H$+23=$E).*

Analyse der Lauftextverschlüsselung

Zum Brechen einer Stromchiffre mit Klartextschlüsselstrom kann man so vorgehen: Man geht zunächst davon aus, dass jeder Kryptotextbuchstabe durch Summation eines Klartext- und Schlüsselstrombuchstabens mit jeweils mittlerer bis hoher Wahrscheinlichkeit entstanden ist. Dies sind beispielsweise im Englischen die Buchstaben E, T, A, O, I, N, S, R, H. Zu einem Teilwort w des Kryptotextes bestimmt man dann alle Paare von Wörtern $(w_1,\ w_2)$ mit $w_1 + w_2 = w$ und $w_1, w_2 \in \{\mathsf{E}, \mathsf{T}, \mathsf{A}, \mathsf{O}, \mathsf{I}, \mathsf{N}, \mathsf{S}, \mathsf{R}, \mathsf{H}\}$. In der Regel ergeben sich nur sehr wenige sinnvolle Paare, aus denen durch Kontextbetrachtungen und Erweitern von w nach links und rechts der Kryptotext entschlüsselt werden kann. Wird die Analyse durch ein Computerprogramm durchgeführt, kann an die Stelle der Kontextbetrachtungen auch die Häufigkeitsverteilung von n-Grammen der Sprache treten. Das Programm wählt dann solche Wortpaare $(w_1,\ w_2)$, die eine hohe Wahrscheinlichkeit haben.

Beispiel 63 *Gegeben ist der Kryptotext* MOQKTHCBLMWXF*... Wir beginnen die Untersuchung mit einer Wortlänge von vier Buchstaben, also $w =$* MOQK*. Der erste Buchstabe* M *kann nur auf eine der folgenden Arten zustande gekommen sein:*

	ABCDE...I...T...Z	*(Klartextzeichen)*
+	MLKJI...E...T...N	*(Schlüsselzeichen)*
=	MMMMM...M...M...M	*(Kryptotextzeichen)*

Es ergeben sich als wahrscheinliche Paare für die Einzelbuchstaben von w:

M:	(E,I)	O:	(A,O)	Q:	(I,I)	K:	(R,T)
	(I,E)		(H,H)				(S,S)
	(T,T)		(O,A)				(T,R)

und damit $(w_1,\, w_2)$ *zu*

w_1	EAIR	EAIS	EAIT	EHIR	...	THIS	...	TOIT
w_2	*IOIT*	*IOIS*	*IOIR*	*IHIT*	...	*THIS*	...	*TAIR*

Als sinnvoll stellt sich also nur die Wahl $w_1 = w_2 =$ THIS *heraus.*

Autokey Chiffren

Kryptotextschlüsselstrom. Diese Systeme bieten eigentlich keinen großen kryptographischen Schutz, da sie ohne Kenntnis des Schlüsselwortes sehr leicht entschlüsselt werden können (falls die Länge des Schlüsselwortes im Verhältnis zur Länge des Kryptotextes relativ kurz ist). Man subtrahiert dazu den Kryptotext y für $d = 1, 2, \ldots$ von dem um d Positionen verschobenen Kryptotext – also $y_{1+\delta}\, y_{2+\delta}\, y_{3+\delta}\, \ldots$ minus $y_1\, y_2\, y_3 \ldots$ –, bis sinnvoller (Klar-) Text erscheint:

$$\begin{array}{rrl} & \mathit{DUMSQMOZKFN...} & \text{(Kryptotext } y\text{)} \\ - & \mathit{DUMSQMO...} & \text{(„Kryptotextschlüsselstrom“)} \\ \hline = & \texttt{....NSCHUTZ...} & \text{(Klartext } x\text{)} \end{array}$$

Klartextschlüsselstrom. Neben der oben beschriebenen Analyse der Lauftextverschlüsselung kann das Brechen der *Autokey*-Systeme mit Klartextschlüsselstrom auch analog zur Kasiski-Methode erfolgen: Sei d die Länge des Schlüsselwortes $k_1 \ldots k_d$. Falls im Klartext die gleiche Buchstabenfolge $x_i \ldots x_{i+\delta-1}$ im Abstand $2d$ auftritt (beispielsweise $d = 3$ und $\delta = 2$),

$$\begin{array}{ccccccccccccccccc|l} & & & & & & & & \downarrow & \downarrow & & \downarrow & \downarrow & & & & & \\ & x_1 & x_2 & x_3 & x_4 & \underline{x_5} & \underline{x_6} & x_7 & x_8 & x_9 & x_{10} & \underline{x_{11}} & \underline{x_{12}} & x_{13} & x_{14} & x_{15} & \ldots & \text{Klartext } x \\ + & k_1 & k_2 & k_3 & x_1 & x_2 & x_3 & x_4 & \underline{x_5} & \underline{x_6} & x_7 & x_8 & x_9 & x_{10} & \underline{x_{11}} & \underline{x_{12}} & \ldots & \text{Klartextschlüsselstrom } kx \\ \hline = & y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & \underline{y_8} & \underline{y_9} & y_{10} & \underline{y_{11}} & \underline{y_{12}} & y_{13} & y_{14} & y_{15} & \ldots & \text{Kryptotext } y \end{array}$$

so tritt im Kryptotext die gleiche Buchstabenfolge im Abstand d auf, d. h. d kann auf diese Art unter Umständen leicht bestimmt werden. Ist d bekannt, so können die Buchstaben $k_1 \ldots k_d$ des Schlüsselwortes der Reihe nach bestimmt werden: Da durch k_i die Klartextzeichen an den Positionen $i,\ d+i,\ 2d+i,\ \ldots$ eindeutig festgelegt sind, kann jedes einzelne k_i unabhängig von den anderen Schlüsselwortbuchstaben durch eine statistische Analyse bestimmt werden.

Bei der dritten Methode *Autokey*-Chiffren mit Klartextschlüsselstrom zu brechen, „rechnet man den Schlüssel aus dem Kryptotext heraus“. Doch zuerst einige allgemeine Betrachtungen zu den Eigenschaften einer *Autokey*-Chiffre mit Klartextschlüsselstrom.

Betrachten wir den Klartext HIERKOMMTEINMUSTER, welcher mit dem Schlüssel *DER* verschlüsselt werden soll:

	HIERKOMMTEINMUSTER	(Klartext)
+	*DERHIERKOMMTEINMUS*	(Schlüsselstrom)
=	*KMVYSSDWHQUGQCFFYJ*	(Kryptotext)

Für eine kryptoanalytische Untersuchung des Geheimtextes nehmen wir nun an, dass die Schlüsselwortlänge $d = 3$ bekannt ist und dechiffrieren den Kryptotext mit einem beliebigen Schlüssel dieser Länge (beispielsweise *AAA*).

	KMVYSSDWHQUGQCFFYJ	(Kryptotext)
−	*AAAKMVOGXPQKBEWPYJ*	(Schlüsselstrom)
=	KMVOGXPQKBEWPYJQAA	(modifizierter Klartext)

Der modifizierte Klartext wird nun mit dem ursprünglichen Klartext verglichen. Dabei fällt auf, dass sich die Differenzen der Buchstaben im Abstand der doppelten Schlüsselwortlänge wiederholen:

h	i	e	r	k	o	m	m	t	e	i	n	m	u	s	t	e	r
K	M	V	O	G	X	P	Q	K	B	E	W	P	Y	J	Q	A	A
3	4	17	23	22	9	3	4	17	23	22	9	3	4	17	23	22	9

Diese Wiederholung besagt aber nichts anderes, als dass bei dem modifizierten Klartext eine gewöhnliche Vigenère-Chiffre vorliegt, die mit einem Schlüssel der Länge $2d$ chiffriert wurde.

Als kryptoanalytische Vorgehensweise ergibt sich daraus folgende Strategie: Da die Länge d des Schlüsselwortes nicht bekannt ist, erzeugt man (wie oben beschrieben) unter Verwendung von unterschiedlichen Werten für $d = 1, 2, 3, \ldots$ aus dem Kryptotext eine Anzahl modifizierter Klartexte, die dann einer Häufigkeitsanalyse mit *doppelter* Schlüssellänge unterzogen werden. Bei dieser Untersuchung sind nur die ersten d Stellen von Bedeutung; sie ergeben das Schlüsselwort, mit dem der ursprünglich gegebene Kryptotext entschlüsselt werden kann.[†]

[†] Unter Verwendung des ursprünglichen Kryptosystems: *Autokey*-Chiffre mit Klartextschlüsselstrom!