Wiederum mag der Verbrecher einen kurzen Schlüssel benutzen, wie 2—3—4, mit dessen Hilfe wird aus den Worten „Don't answer“:

D O N T A N S W E R
2 3 4 2 3 4 2 3 4 2
F R R V D R U Z I T

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

Abb. 2. Vigenères Tafel, nach der irgendein Alphabet das normale in der ersten Zeile ersetzen kann; eine Zahl zeigt dem Empfänger an, welche Zeile benutzt wurde.

Eine Variation hiervon ist das Schlüsselwort, das lang oder kurz sein kann. Jeder Buchstabe nimmt seinen alphabetischen Wert nach der entsprechenden Stellung derer, die das Schlüsselwort bilden. Zum Beispiel:

Botschaft	D	O	N	T	A	N	S	W	E	R
Schlüsselwort	F	O	R	G	E	T	F	O	R	G
Wert in Zahlen	6	15	18	7	5	20	6	15	18	7
Umstellung	j	d	f	a	j	n	y	l	w	y

Solche Kryptogramme können nicht entziffert werden, wenn die Botschaft so kurz ist, daß sie nur ein oder zwei Worte enthält.

Natürlich ist der erste Schritt, die vom Schreiber gebrauchte Sprache zu entdecken. Die einzig wirksame Methode für diesen Zweck besteht in der Klassifizierung der wiederkehrenden Buchstabengruppen. Hat man sie herausgeschält, so stellt man die Häufigkeit fest, mit der verschiedene Buchstaben wiederholt sind, und vergleicht sie mit den für jede Sprache zusammengestellten Durchschnittsskalen, bis die Stellung und Wiederkehr eines Buchstabens oder einer Gruppe zum wahrscheinlichen Stück eines Wortes wird. Eine lange und mühselige Aufgabe! So wurde das Rätsel der berühmten Chiffre, die Frankreichs Könige gebrauchten, erst kürzlich gelöst; sie hatte den unablässigen Anstrengungen der Sachverständigen mehr als ein Jahrhundert Trotz geboten.

Es gibt jedoch eine auf jede Geheimkorrespondenz anwendbare Grundregel. Da die europäischen Alphabete auf sechsundzwanzig Buchstaben beschränkt sind, muß irgendeine Serie von Worten dieselben charakteristischen Kombinationen und dieselbe perio-