Der Kasiski-Test

Bestimmung des Schlüsselwortes bei bekannter Schlüssellänge

Stellen wir uns vor, wir haben den untenstehenden verschlüsselten Text abgefangen.

```
YMVCZAIIHMVBOMIINBKVBMRVILIUZAXVSBIJYMRWZPPVM
```

Wir wissen über ihn, dass er auf **Deutsch** verfasst ist und mit dem **Vigenère-Verfahren** verschlüsselt wurde. Zudem wissen wir, dass der Schlüssel die **Länge 4** hat. Wir müssten jetzt nur noch wissen, welche vier Buchstaben das Schlüsselwort bilden…

Die Idee: Wir teilen den Text in Stücke der Länge 4 auf und schreiben diese untereinander:

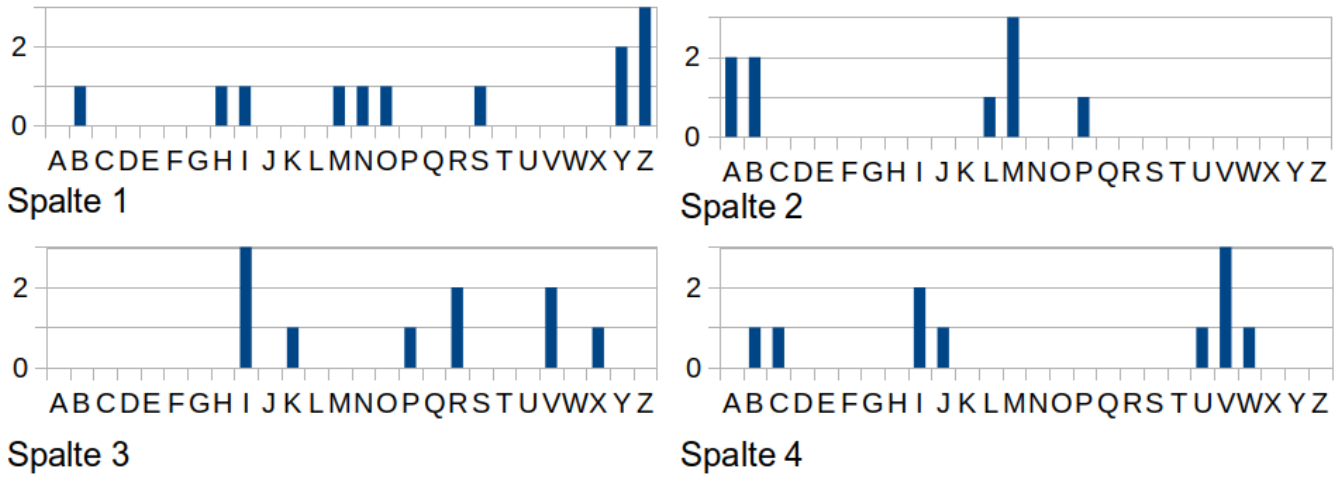
Y	M	V	C
Z	A	I	I
H	M	V	B
O	M	I	I
N	B	K	V
B	M	R	V
I	L	I	U
Z	A	X	V
S	B	I	J
Y	M	R	W
Z	P	P	V
M			

Überlegung 1: Was haben die Buchstaben in einer Spalte gemeinsam? Wie sind sie beim Verschlüsseln aus dem Klartext entstanden?

Überlegung 2: Wir haben eine charakteristische Eigenschaft deutscher Texte kennengelernt. Wie kann diese einen Hinweis auf den ersten, zweiten, dritten und vierten Schlüsselbuchstaben geben?

Hilfestellung:

Die folgenden Häufigkeitsdiagramme zeigen die Anteile der Buchstaben in den jeweiligen Spalten:



Ermittle das Schlüsselwort und entschlüssle den Geheimtext.

Hilfestellung Vigenere-Quadrat:

Schlüsselbuchstaben in dieser Spalte suchen --->		Klartextbuchstaben in dieser Zeile suchen --->																									
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
		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
0	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

↑ Chiffretextbuchstaben im Inneren der Tabelle suchen ↑

Bestimmung des Schlüsselwortes bei bekannter Schlüssellänge

Wenn die Schlüssellänge bekannt ist, kann die Häufigkeitsanalyse also helfen, das Schlüsselwort zu

finden und auf diese Weise die Verschlüsselung zu brechen. Leider ist die Schlüssellänge meist nicht wie im ersten Beispiel bekannt - es wäre also sehr hilfreich, wenn es eine Möglichkeit gäbe, die Schlüssellänge zu ermitteln.

Vorüberlegung

Der Text `Die Lilie, die Rose und die Tulpe` wurde mit dem Schlüssel BLAU verschlüsselt. Im Schlüsseltext kommt es zu einer Wiederholung. Woran liegt das? Warum wird das dritte `die` anders verschlüsselt als die ersten beiden?

D	I	E	L	I	L	I	E	D	I	E	R	O	S	E	U	N	D	D	I	E	T	U	L	P	E
B	L	A	U	B	L	A	U	B	L	A	U	B	L	A	U	B	L	A	U	B	L	A	U	B	L
E	T	E	F	J	W	I	Y	E	T	E	L	P	D	E	O	O	O	D	C	F	E	U	F	Q	P

Schlüssellänge finden

Stellen wir uns vor, wir haben den untenstehenden verschlüsselten Text abgefangen.

```
PMRVDIPLYHIZYLYEOYRUPMRVVEXVKYRUPMRYLLR
```

Wir wissen über ihn, dass er mit dem **Vigenère-Verfahren** verschlüsselt wurde.

- Markiere auffällige Wiederholungen von Bigrammen oder Trigrammen im Geheimtext farbig.
- Nutzen die gefundenen Auffälligkeiten, um eine Vermutung zur Schlüssellänge zu erhalten.
- Erläutere, wie man anhand von Auffälligkeiten im Geheimtext einen Hinweis auf die Schlüssellänge erhalten kann.
- Kannst du das Codewort finden? Warum klappt das nicht so gut?

Lösung:

Schlüssel: LEER, du kannst das hier überprüfen: https://www.cryptool.org/de/cto/vigenere

From:
https://info-bw.de/ -

Permanent link:
https://info-bw.de/faecher:informatik:oberstufe:kryptographie:vigenere:kasiski:start?rev=1645727189

Last update: **24.02.2022 18:26**