

Aufgabe In der folgenden Tabelle sind die Häufigkeiten angegeben.

1

A	B	C	D	E	F	G	H	I
6,48 %	16,3 %	6,88 %	1,18 %	0,20 %	0,59 %	1,96 %	0,39 %	3,14 %

J	K	L	M	N	O	P	Q	R
0,39 %	7,66 %	6,29 %	5,30 %	3,14 %	0,98 %	0,00 %	9,62 %	4,72 %

S	T	U	V	W	X	Y	Z
6,48 %	1,18 %	2,55 %	2,16 %	2,75 %	2,36 %	1,96 %	5,30 %

Der Buchstabe mit dem höchsten Anteil kann leicht zugeordnet werden. So entspricht das **B** dem Klartext **E**. Besonders häufig treten auch, mit absteigender Häufigkeit, **Q**, **K**, **C**, **A**, **S** und **L** auf. Sie können einem der Buchstaben **N**, **I**, **S**, **R**, **T** oder **A** zugeordnet werden. Es lässt sich erschließen, dass **Q** dem Klartextbuchstaben **N** entspricht, weil die Häufigkeit einen großen Abstand zu den anderen Häufigkeiten besitzt. Wie die Zuordnung für die anderen Buchstaben genau aussieht, wissen wir jedoch noch nicht.

Im Text kommen fünf verschiedene Doppelbuchstaben vor. Dies sind **QQ**, **AA**, **LL**, **YY** und **WW**. Da **Q** bereits **N** zugeordnet wurde, muss es sich bei **AA** um **S** handeln, weil **SS** eigentlich am häufigsten vorkommen sollte.

Wir wissen also, dass es sich bei **A** um **S** handelt und können uns deswegen anschauen, welche Bigramme dem **A** häufig folgen. Dabei muss es sich dann um das **SCH** handeln. Dabei können wir Bigramme auslassen, bei denen ein Buchstabe bereits entziffert ist. **ANR** taucht im gesamten Text fünfmal auf. Außerdem treten **NR** insgesamt vierzehnmal gemeinsam im Text auf. Die zweithäufigste Kombination **AKM** finden wir dreimal im Text, allerdings **KM** nur zusammen mit **A**. Dabei kann es sich also nicht um **SCH** handeln. Also muss **ANR** die Klartextbuchstaben **SCH** verschlüsseln.

Von den häufigsten Buchstaben bleiben noch **K**, **C**, **S** und **L** bzw. **I**, **R**, **T** oder **A**. Dies können wir uns für die weitere Kryptoanalyse merken.

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			N		B		V	R			X		Y	Q					A				D			G



Aufgabe

2

Durch das sorgfältige Durchgehen des Textes fallen z.B. diese Dinge auf:

- Insgesamt viele kurze Wörter beginnen mit **Z** und stehen häufig vor großgeschriebenen Wörtern. Also kann es sich dabei nur um Artikel handeln, die eigentlich mit **D** beginnen.
- In Zeile sieben steht ein Wort aus zwei Buchstaben **Ai**. Da wir bereits wissen, was **A** verschlüsselt, kann es sich dabei nur um das Wort **So** handeln. Die Zuordnung von **I** zu **O** passt auch, da **IB** häufiger vorkommt, dabei handelt es sich um **OE**, also den Umlaut **Ö**, der in der Kryptologie häufig nicht vorkommt.
- In der ersten Zeile steht **zcbabq**, was aufgrund der bisherigen Ergebnisse zu **d_esen** entschlüsselt wird, also muss es sich dabei um **diesen** handeln. Dies passt auch gut in den häufig vorkommenden Artikel **zcb**, also **die**.
- Im Text findet sich zweimal das Wort **sqz**, das bereits als **_nd** entschlüsselt werden kann. Deswegen muss **S** zum Klartextbuchstaben **U** gehören. Dadurch wird aus **zs** auch **du** und aus **Qsq** **Nun**.

Natürlich können auf diese Weise auch noch viel mehr Buchstaben aufgedeckt werden. Dadurch sieht die Ersetzungstabelle insgesamt so aus:

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

Daraus ergibt sich der Text:

Wenn du diesen Text entschlüsseln könntest, beherrschst du die Kryptoanalyse richtig gut. Nun wird dich keine monoalphabetische Verschlüsselung mehr aufhalten können.

Der Trick dabei ist, nicht nur auf die Häufigkeiten der Buchstaben zu achten, sondern auch das Wissen über die Sprache, die Erfahrungen aus der Kryptologie und deine Intuition zu nutzen. So kannst du zum Beispiel Bigramme und kurze Wörter verwenden, um Buchstaben festzulegen. Deine Intuition hilft dir Buchstaben, Wörter oder ganze Sätze zu erraten. Je mehr Geheimtexte du bereits geknackt hast, desto schneller kommst du an das Ziel.