Station 3 – Vigenère

Hintergrund

Die Vigenère-Verschlüsselung stammt aus dem 16. Jahrhundert. Im Gegensatz zur Caesar-Verschlüsselung nutzt sie nicht nur ein Alphabet, sondern mehrere, um aus einem Klartext einen Geheimtext zu erstellen.

Seit der Antike ist viel Zeit vergangen und wie in vielen Bereichen der Wissenschaft gab es bis zum Mittelalter kaum wirkliche Fortschritte. Dies änderte sich, als durch die Stadtstaaten in Italien des Mittelalters viele Botschafter an anderen Höfen verweilten und geheim mit ihren jeweiligen Herren kommunizieren mussten. Es entstand ein reger Wettbewerb beim Verschlüsseln und Entschlüsseln von Nachrichten. Der arabische Gelehrte al-Kindī entwickelte im 9. Jahrhundert die Häufigkeitsanalyse als kryptografisches Verfahren. Erst viele Jahre später kam das Verfahren nach Europa und ermöglichte es, die bis dahin üblichen Verfahren mit Leichtigkeit zu brechen.

Das Wissen darum war aber nicht an allen Höfen gleichermaßen verbreitet. So versuchte der spanische König Philipp II. seine französischen Rivalen beim Vatikan anzuschwärzen. Der Franzose Viète müsse mit dem Teufel persönlich im Bunde sein, da er die spanischen Geheimbotschaften so leicht entschlüsseln könne. Der Vatikan und andere Länder konnten das aber genauso. Somit machte er Spanien zum Gespött an europäischen Höfen.

Da die Vigenère-Verschlüsselung nicht nur ein Alphabet, sondern mehrere nutzt, scheiterte die Häufigkeitsanalyse. Das Verfahren galt zur damaligen Zeit als “le chiffre indéchiffrable”, also als unentzifferbare Chiffre.

Erst 1854 fand der englische Wissenschaftler Charles Babbage eine Möglichkeit, die Methode zu knacken. Er veröffentlichte seine Arbeit aber nie. Die erste öffentlich bekannte Methode geht auf den Infanteriemajor Friedrich Wilhelm Kasiski zurück, der sie 1863 in seinem Buch „Die Geheimschriften und die Dechiffrir-Kunst“ beschrieb. Noch heute heißt das Verfahren Kasiski-Test.

Prinzip

Mit der Vigenère-Verschlüsselung wurden einige wichtige Verbesserungen an den üblichen Ceasar-Verschlüsselungen und ihren Abwandlungen vorgenommen, um die Kryptoanalyse mittels Häufigkeitsanalyse zu unterbinden. Um zu verhindern, dass die Häufigkeit der Buchstaben erhalten bleibt, wird nicht nur eines sondern mehrere Geheimtextalphabete verwendet. Daher ist die Viginère-Verschlüsselung eine polyalphabetische Verschlüsselung.

Das Ganze funktioniert wie folgt. Es wird ein Passwort oder ein –satz ausgemacht. Dieser dient als geheimer Schlüssel zwischen den Kommunikationsteilnehmerinnen und –nehmern. Der erste Buchstabe des Schlüssels gibt an, wieweit der erste Buchstabe des Klartextes bei einer Caesar-Verschlüsselung verschoben wird. Der zweite Buchstabe des Schlüssels für den zweiten Buchstaben des Klartextes und so weiter. Sind alle Buchstaben des Schlüssels aufgebraucht, beginnt man den Schlüssel wieder von vorne.

Beispiel

Verschlüsselung

Wir haben den geheimen Schlüssel “NUERNBERG” ausgemacht. Nun möchte ich den folgenden Text verschlüsseln.

“Seismosaurus bedeutet Erdbebenechse”

Um die Verschlüsselung etwas einfacher zu machen, kann ich den geheimen Schlüssel über den Klartext schreiben und ihn wiederholen, bis ich genügend Buchstaben für den Text habe. Wenn der Klartext ein Leerzeichen hat, füge ich auch in den Schlüssel eines ein.

```
Schlüssel:  NUERNBERGNUE RNBERGNU ERNBERGNUERNB
Klartext:   Seismosaurus bedeutet Erdbebenechse
Geheimtext: Fym
```

Daraus kann ich direkt ablesen, mit welcher Caesar-Verschlüsselung ich welchen Klartextbuchstaben verschlüsseln muss.

Das S am Anfang wird so verschlüsselt, dass ein A ein N wird, da N der zugehörige Buchstabe aus dem Schlüssel ist. Also ein F.

```
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 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
```

Das e wird so verschlüsselt, dass ein A ein U wird, da U der zugehörige Buchstabe aus dem Schlüssel ist. Also ein y.

```
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: 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
```

Beim i wird das Alphabet so weit verschoben, dass ein A ein E ergibt, da der nächste Buchstabe des Schlüssels ein E ist. Somit ergibt sich für i ein m.

```
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: 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
```

Wenn wir dieses Verfahren fortsetzen, erhalten wir für den Beispieltext folgenden Geheimtext.

```
Schlüssel:  NUERNBERGNUE RNBERGNU ERNBERGNUERNB
Klartext:   Seismosaurus bedeutet Erdbebenechse
Geheimtext: Fymjzpwraeow sreilzrn Iiqciskaygyff
```

Entschlüsselung

Bei der Entschlüsselung gehen wir nach dem gleichen Schema vor, müssen aber wie bei der Caesarverschlüsselung die Reihenfolge von Klartext und Geheimtext tauschen.

```
Schlüssel:  NUERNBERGNUE RNBERGNU ERNBERGNUERNB
Geheimtext: Fymjzpwraeow sreilzrn Iiqciskaygyff
Klartext:   Sei
```

Wir beginnen mit dem ersten Geheimtext-Buchstaben F und dem zugehörigen Schlüssel-Buchstaben N. Wir verschieben das Alphabet soweit, dass das A vom Kl

```
Geheimtext: 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
Klartext:   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
```

Beim zweiten Buchstaben des Geheimttextes y haben wir den Schlüssel-Buchstagen U. Also verscieben wir das Alphabet soweit, dass das A einem U entspricht.

```
Geheimtext: 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
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
```

Dies können wir nun für Buchstaben des Geheimtextes wiederholen.

```
Schlüssel:  NUERNBERGNUE RNBERGNU  ERNBERGNUERNB
Geheimtext: Fymjzpwraeow sreilzrn Iiqciskaygyff
Klartext:   Seismosaurus bedeutet Erdbebenechse
```

Vigenère-Quadrat

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Um die Ver- und Entschlüsselung zu vereinfachen, wurde das Vigenère-Quadrat als Hilfsmittel erfunden. In der obersten Zeile ist das Klartextalphabet. In der linken Zeile das Gemheimtextalphabet des jeweiligen Zeichens.

Beim Verschlüsseln eines Buchstaben suche ich die Kreuzung der Spalte des Klartext-Buchstabens und der Zeile des Schlüssel-Buchstabens. Dort befindet sich der Geheimtext-Buchstabe. Beim ersten Buchstaben unseres Beispieltextest gehe ich zu Spalte S. Dann suche ich die Zeile N. Die Zelle S/N beinhaltet dann den gesuchten Buchstaben F.

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Beim Entschlüsseln gehe ich umgekehrt vor. Ich habe den Geheimtext-Buchstaben F und suche die passende Zeile mit dem gleichen Buchstaben. Dann wähle ich die Zeile mit dem Schlüssel-Buchstaben N. Die Zelle N/F beinhaltet dann den gesuchten Klartextbuchstaben S.

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Angriffe

Brute-Force

Reines Ausprobieren ist bei Vigenère-Verschlüsselungen sehr aufwändig, da nicht nur ein Alphabet, sondern eine unbekannte Anzahl geknackt werden müssten. Je nach Länge des Schlüssels wird eine andere Anzahl von Alphabeten verwendet.

Häufigkeitsanalyse

Bei Viginère kann die einfache Analyse der Häufigkeit der Buchstabe nicht angewandt werden. Stattdessen muss zunächst die Länge des Schlüssels ermittelt werden.

In Sprachen kommen bestimmte Kombinationen von Buchstaben häufig vor. Im Deutschen zum Beispiel “der”, “die” oder “und” aber auch Teile von Wörtern. Weil sie so häufig vorkommen, können wir annehmen, dass diese Buchstabenkombinationen auch mehrmals mit dem gleichen Teil des Schlüssels verschlüsselt werden. Es wird also mehrmals die gleichen Buchstabenfolgen im Geheimtext geben.

Nun suchen wir im Geheimtext nach Wiederholungen von Buchstabenkombinationen. Möglichst lange, aber auch drei oder zweistellige gehen.

Nehmen folgende verschlüsselten Auszug aus der Wikipedia.

```
SqdmuguhsOaqudndmkaeizzduumksebqsSobisdnhkgdiqmmtnsWqdgpvnndtzAzsxthjubjdk
evbdOiohzhsiadhttbvzdtzLhtimcdsYigqhjvcdriamzcwodvitadmaaacheIwlzttqmRutlh
saaqdmpdxtkatzvtrsmCdrCildihbudrbcskirpzdlimqcitiotlxabgeEqyyaecfkitadndtz
chezikzbgmrhsrpdOiibzhnrphtsphtlBtqroittdmtwiksecvdaecPdeeimhfnjzrdiiikseg
aadkpvmseOcszttvvheDthuecwdkZlqdaeavRzlowcdrHkgvexvdrcwuzkzSmqkivcqhsrpdmF
dkzbcxizdhcthbhtNkzdtvaqoimrhnsadhtsmqZniqjdvtzaqexbdsDpXhyzpjdhstpqgowmqS
ebxdqaicqfeqibjecedqdtvrnlabdvahqmcecedmivasdnWitrhptsdnbwdflxkgvagetqdtah
dacnzmghdnqbtzdhttbtmdjvfdbpkjdnoclnegbkhcwmmAatkjdrvmaqarpsaihmhmexodmegP
zmdlmqjsoedhgsmqOiohzlarpdqdtzOhzoihnldmmssiimcdtzcdnImhfsttartwmqrtttksej
vcaeamfse
```

Beispielsweise finden sich die Kombinationen **OIOHZ**, **DHTTB** und **HSRPD** jeweils zwei Mal im Text.

Als nächstes versuchen wir die Länge des Schlüssels herauszufinden. Wir zählen den Abstand zwischen dem Beginn zweier gleicher Buchstabenkombinationen. Zwischen dem a des ersten **OIOHZ** und dem des zweiten liegen 530 Zeichen. Bei **DHTTB** sind es 545 Zeichen und bei **HSRPD** sind es 130. Die Schlüssellänge muss ein gemeinsamer Teiler der ermittelten Abstände sein, denn damit es Wiederholungen der Buchstabenkombination geben kann, muss der Schlüssel auch wiederholt worden sein. Der größte gemeinsame Teiler von 530, 545 und 130 ist 5. Daher gehen wir davon aus, dass der geheime Schlüssel des Textes 5 Buchstaben lang ist.

Wenn wir von einer Schlüssellänge von 5 ausgehen, können wir den Geheimtext so analysieren, als hätten wir fünf verschiedene Caesar-Verschlüsselungen vorliegen. Diese können wir mit der Häufigkeitsanalyse der Buchstaben knacken.

```
SqdmuguhsOaqudndmkaeizzduumksebqsSobisdnhkgdiqmmtnsWqdgpvnndtzAzsxthjubjdk
evbdOiohzhsiadhttbvzdtzLhtimcdsYigqhjvcdriamzcwodvitadmaaacheIwlzttqmRutlh
saaqdmpdxtkatzvtrsmCdrCildihbudrbcskirpzdlimqcitiotlxabgeEqyyaecfkitadndtz
chezikzbgmrhsrpdOiibzhnrphtsphtlBtqroittdmtwiksecvdaecPdeeimhfnjzrdiiikseg
aadkpvmseOcszttvvheDthuecwdkZlqdaeavRzlowcdrHkgvexvdrcwuzkzSmqkivcqhsrpdmF
dkzbcxizdhcthbhtNkzdtvaqoimrhnsadhtsmqZniqjdvtzaqexbdsDpXhyzpjdhstpqgowmqS
```

ebxdqaicqfeqibjecedqdtvrnlabdvahqmcecedmivasdnWitrhptsdnbwdflxkgvagetqdtah
dacnzmghdnqbtzdhttbtmdjvfdbpkjdnoclnegbkhcwmmAatkjdrvmaqarpsaihmhmexodmegP
zmdlmqjsoedhgsmqOiohzlarpdqdtzOhzoihnldmmssiimcdtzcdnImhfsttartwmqrtttksej
vcaeamfse

Nehmen wir zuerst die Buchstaben 1, 6, 11...

SgadiubbhqsptxbvoittiYjiwtaIttadtsChbritxEettzgrirpttwccijigpOtDclaoHxwSvr
dxcttissitxpptwbiqctahcvWpbxgtchttjpogwtvrhxglosortoditItwtja

Das T kommt mit großem Abstand am häufigsten vor. Wenn wir nun in dem Vigenère-Quadrat in der Spalte E nachsehen, in welcher Spalte E mit einem T ersetzt wird, erhalten wir als ersten Buchstaben des Schlüssels ein P.

Nun betrachten wir die Buchstaben 2, 7, 12...

quqmzmqikmWvztjbhabzmivaoaawqlqxzmibcpmiaqcazimpbphqtivPmziavcvtwqvwkvumcp
kitNvmamqzbXjpmxcievbqeaitwkeandzbvkcbmkmpmoPmemhpzimizmtmtvm

Auch hier ist die Häufigkeitsanalyse relativ eindeutig und der Buchstabe M ist der häufigste. Laut Vigenère-Quadrat hätten wir damit den Schlüssel-Buchstaben I.

Als nächstes die Buchstaben 3, 8, 13...

dhukzkssgmqnAhddzdvLcgcmddclmhdtvCluszqobyfdckrdzhtrdkddhrkamsvhddRcgdzqqd
zzhkardqjadhdqqdqbdrdmdstsdgthzndtfjlkmjashdzqdqzdOhmmchaqkcf

Mit über 20 % ist D der häufigste Buchstabe. Aus dem Vigenère-Quadrat lesen wir den Buchstaben Z als dritten Schlüssel-Buchstaben ab.

Nun zu den Buchstaben 4, 9, 14...

msdadsSddtdnzjkOhhzhdqdzvmhzRsmktdddkdctgyknhzhOhtlomsaefdsdszhukazdvrkkhmbdbzqhhZd
qsyhgSqfjqnvcmdrdfvqdmqhmddnhAdqammmjhOlqhnscdfrrsas

Diesmal ist die Verteilung nicht ganz so eindeutig aber mit 17 % ist wieder das D am häufigsten. Daraus ergibt sich wieder ein Z als Schlüssel-Buchstabe

Zum Schluss prüfen wir die Buchstaben 5, 10, 15...

uOneueoningdsueistdtshrciaetuaparririlileaidebsinsBiteeenieketeeZelreczisF
chhdontnveDzsoeaeedlaeinhnladagbtdbnecaraieedsgiadzlsdnstteee

Hier kommt das E am häufigsten vor, was uns ein A als letzte Buchstaben des Schlüssels liefert.

Somit lautet der geheime Schlüssel für den Text **PIZZA**.

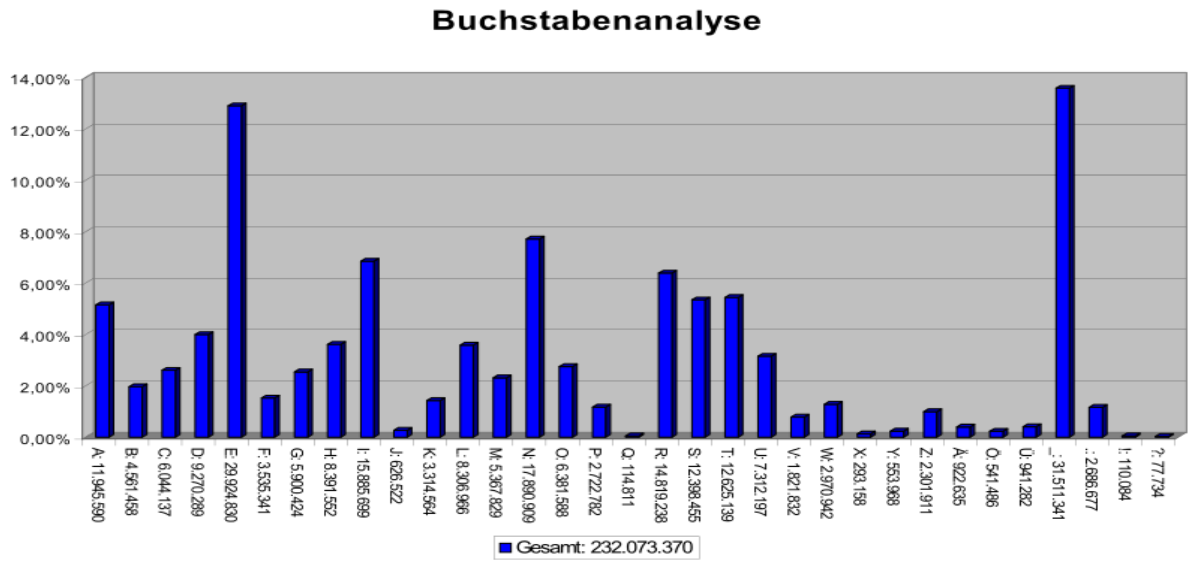
Nun können wir den Schlüssel prüfen, indem wir die Buchstaben nach und nach ersetzen. Es ergibt sich folgender Text:

DienurmitOlivenoelbetraeufeltemitTomatenscheibenundOreganooderBasilikumbelegtePizzaistseitet
waderMittedesJahrhundertsnachgewiesenalsdieTomateinSueditalienpopulaerwurdeDerNameistver
mutlichaelterdieapulischePizzapuglieseoderdiekalabresischePittainchiusazumBeispielenthaltennebe
nHefeteignurseitaltersbekannteZutatenwieOlivenoelZwiebelnSalzoderSchweineschmalzDerligurische
nFocacciaaehnlicheFladenbrotesindseitderAntikeverbreitetDaPizzabeisehrhoherTemperaturgebacke
nwerdensolltewasindenwenigstenHaushaltenmoeglichwarwurdesieanfangsvorbereitetundungeback

enzumoertlichenBaeckergebrachtbiseineigenerHandwerkszweigderPizzamacherderPizzaioloentstanddenTeigselbstherstellteundbelegte

Wir ergänzen noch ein paar Leer- und Satzzeichen und sind fertig mit dem Knacken:

Die nur mit Olivenoel beträufelte, mit Tomatenscheiben und Oregano oder Basilikum belegte Pizza ist seit etwa der Mitte des 18. Jahrhunderts nachgewiesen, als die Tomate in Sueditalien populaer wurde. Der Name ist vermutlich aelter – die apulische Pizza pugliese oder die kalabresische Pitta inchiusa zum Beispiel enthalten neben Hefeteig nur seit alters bekannte Zutaten wie Olivenoel, Zwiebeln, Salz oder Schweineschmalz. Der ligurischen Focaccia aehnliche Fladenbrote sind seit der Antike verbreitet. Da Pizza bei sehr hoher Temperatur gebacken werden sollte, was in den wenigsten Haushalten moeglich war, wurde sie anfangs vorbereitet und ungebacken zum oertlichen Baecker gebracht, bis ein eigener Handwerkszweig der Pizzamacher, der Pizzaiolo, entstand, der den Teig selbst herstellte und belegte.



Quelle: Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Alphabet_haufigkeit.svg

Ausprobieren

Verschlüssele oder Entschlüssele die Beispiele

Um ein bisschen Übung zu bekommen haben wir drei Beispieltexte vorbereitet. Da Umlaute etc. Eine Vergrößerung der Viginère-Quadrate nötig machen würde und es so schon recht umfangreich ist, wurden Umlaute wie im Kreuzworträtsel ersetzt.

1. Nimm dir ein Viginère-Quadrat
2. Suche dir einen Klartext aus und führe die Viginère-Veschlüsselung mit dem angegebenen Schlüssel durch
3. Vergleiche dein Ergebniss mit dem Geheimtext auf der Rückseite
4. Versuche nun einen der Geheimtexte mit dem angegebenen Schlüssel zu entschlüsseln

Knacke den Geheimtext

Als zweiten Versuch kannst du dich an die Entschlüsselung des Geheimtextes ohne Klartext machen.

Hierbei kannst du ein paar Hilfsmittel am Computer benutzen. Der Geheimtext ist am Computer im Editor geöffnet. Mit der Viginère-Analyse kannst du die Häufigkeit und den Abstand von Buchstabenkombinationen herausfinden und anschließend das Codewort ermitteln.

Viginère-Quadrat

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Klartext – Der Froschkönig

In den alten Zeiten, wo das Wuenschen noch geholfen hat, lebte ein Koenig, dessen Toechter waren alle schoen; aber die juengste war so schoen, daß die Sonne selber, die doch so vieles gesehen hat, sich verwunderte, sooft sie ihr ins Gesicht schien. Nahe bei dem Schlosse des Koenigs lag ein großer dunkler Wald, und in dem Walde unter einer alten Linde war ein Brunnen; wenn nun der Tag recht heiss war, so ging das Koenigskind hinaus in den Wald und setzte sich an den Rand des kuehlen Brunnens - und wenn sie Langeweile hatte, so nahm sie eine goldene Kugel, warf sie in die Hoehe und fing sie wieder; und das war ihr liebstes Spielwerk.

Schlüssel: GOLD

Geheimtext – Der Froschkönig

O b o h t o w w k b K h o h p q c c o d y K f h t g n k k b y r i v r h n c w i k b s d z z p e z s p

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

g f d r y q s r k b o d j w p V u b y h y s w e k f o l k r z f n g z y o s w h y u p v k v p q n o e v

o q s y k f h x t r p u z s d r u t e v o s t k x w y v M s d l i v e v i v t h t B l k k p p l j s x V i v

w r y g p g k g V r k b t j y z l j k w y j x c p u j i y n r s c Z g z o x t r t q j s x Z g z o h a b e h

x s t q k f l o z s y O o b o h c o c h o b M u a b y h t k p q t b f q j s c W g u c h i v e k k w d v

c o c v u u t q m r l v Q c p q o u d n o b o k o b l x y w y g k b H d r r f q j g p w f h p v o q s

d t r p q X o y g j s d n a s s o k b M u a b y h t g f q j k p q t g t h R o y j k k p l r s s d z h p v

u b l k s g t h k w y h m c w g k b p N a u p o c o c i y w p l t r t h N c p k k i y g l w y j y w p

z o s o h x i y g j o d z g f t k x z t h h g e h y G a l k z h h x y

Schlüssel: GOLD

Klartext – Von einem, der auszog, das Fürchten zu lernen

Ein Vater hatte zwei Soehne, davon war der aelteste klug und gescheit, und wusste sich in alles wohl zu schicken. Der juengste aber war dumm, konnte nichts begreifen und lernen, und wenn ihn die Leute sahen, sprachen sie: "Mit dem wird der Vater noch seine Last haben!" Wenn nun etwas zu tun war, so musste es der aelteste allzeit ausrichten; hiess ihn aber der Vater noch spaet oder gar in der Nacht etwas holen, und der Weg ging dabei ueber den Kirchhof oder sonst einen schaurigen Ort, so antwortete er wohl: "Ach nein, Vater, ich gehe nicht dahin, es gruselt mir!" Denn er fuerchtete sich. Oder wenn abends beim Feuer Geschichten erzaehlt wurden, wobei einem die Haut schaudert, so sprachen die Zuhoerer manchmal: "Ach, es gruselt mir!" Der juengste sass in einer Ecke und hoerte das mit an und konnte nicht begreifen, was es heissen sollte. "Immer sagen sie, es gruselt mir, es gruselt mir! Mir gruselt's nicht. Das wird wohl eine Kunst sein, von der ich auch nichts verstehe."

Schlüssel: ANGST

Geheimtext – Von einem, der auszog, das Fürchten zu lernen

E v t N t t r x z t t g k r p e v Y g x h a k v t v b t o t r q k j t e y z w l t r q d n g h t v z e f i z x

i g a f w w h y k m e f o u a i a g d e e f c g a l m a k v h v i c x n Q k j c u r t y l t r g t x r j g j

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

f g z x n f v j t c u k f l i r S a m d r s o b r q j w k V n z w k n b i z l e v t w E a f z z t b r t O x

n a t m g e g c s l z h z m g w n x k h m h y k m e r y v x r n k d m e f z w t l y f w b t n a k k i

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

p a f n g e e a a f w d r x O x g t o f z d n h w b u r h w k d r t C b r p n z h f b j w k s b t k m

e v t w g s p n s n r v m w g O e z k h a a z o h r g k l x e e c g a l N i z g e v t N t t r x a v h t k

z x n v i z m d n n a g e f m j n s r r l f i e J w g n r x x n e e i z m e g k k b c u U v x r j k f g a

o k f w s o k a f F r a w k G r y u a i p n l x n r x r t e u r l p u e j w g w b h w b e v t w f d v k

Z t u g y u a a h j w k t f u k i r n i z x n q o w S u u u w k e e s s g c u s s e A p n w l g e a k x

l g s a k D r x b n e a m k m e f g k l i a k a g e e K u d e h t v a o r x l x d n y e b t n t m g d x

u f g t r t a v h g h w z r r o x x n j g k x s u k a l s r t k h l y z w B m z k j l a t k f l i r k k z r h

y w e t z o j x s t x m l e y z e b r Z o j z r h y w e t f t a v h g J s l w v x v p o u r w b n r Q m

g s g y w b n i u f w e e o u a a h i z g i p n l l v r x k m e u k

Schlüssel: ANGST

Klartext – Der Wolf und die sieben jungen Geißlein

Es war einmal eine alte Geiss, die hatte sieben junge Geisslein, und hatte sie lieb, wie eine Mutter ihre Kinder lieb hat. Eines Tages wollte sie in den Wald gehen und Futter holen, da rief sie alle sieben herbei und sprach: "Liebe Kinder, ich will hinaus in den Wald, seid auf eurer Hut vor dem Wolf, wenn er hereinkommt, so frisst er euch mit Haut und Haar. Der Boesewicht verstellt sich oft, aber an seiner rauhen Stimme und an seinen schwarzen Fuessen werdet ihr ihn gleich erkennen." Die Geisslein sagten: "Liebe Mutter, wir wollen uns schon in acht nehmen, Ihr koennt ohne Sorge fortgehen." Da meckerte die Alte und machte sich getrost auf den Weg.

Schlüssel: WOLF

Geheimtext – Der Wolf und die sieben jungen Geißlein

A g h f n s t s i o w j e b p f h h p L a w d x z w p m w h e j o w p g a b u z j u p L a w d x h s t

s q b o m w h e j o w p q e s m b e s p n j s X z p h p w e v c j G w y i a f w n a p s f p S t s a g

E f c s d b k z w y a g t j e b o j j K l q z u p m a b f s z T f y p s c m k z p s z o c n a t d n a o

w q a g t j x s y m a f m j e i y i o d c f y v W n a p p P e b o j n w n m s w w q d w y f q g t s z

s y B w z o x a w o f q t p z n s c M q h g t n r p r S c w k s s y s a f s j n s t s g c x r p g z k n

w d x p s c j q q s r e h S f q h f s z V l f n R p w X c p x a k t h d h g j n g e j h z e x e q s t b h

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

s e n d f t m j u w j e q s j n y p s j s y I e s R j e g d q a w y x w u e j j Z t j x s X z p h p w s w

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

Z o x j y y p w p s o n a O w y a i y i i o n m p s d n y v r j p f z x p o f k z s y B a u

Schlüssel: WOLF