Themen

Häufigkeitsanalyse

Bei monoalphabetischen Verschlüsselungen wie der Caesar-Verschlüsselung wird jeder Buchstabe des Klartextalphabets durch einen Buchstaben oder ein Symbol des Geheimalphabets ersetzt.

Die einzelnen Buchstaben einer Sprache kommen in einem Text unterschiedlich häufig vor. In deutschen Texten kommt beispielsweise das „E“ doppelt so häufig vor wie das „I“ und zehnmal so häufig wie das „K“.

Das nutzt man bei der Häufigkeitsanalyse. Der Erfinder dieses Verfahren zum Brechen monoalphabetischer Verschlüsselungen ist der arabische Gelehrte al-Kindi (800–873). Er gilt damit als einer der Pioniere der Kryptoanalyse, also der Kunst, einen Geheimtext ohne Schlüssel zu entziffern.

Bei der Häufigkeitsanalyse werden die einzelnen Buchstaben des Geheimtextes gezählt und ihre Häufigkeit innerhalb des Geheimtextes ermittelt.

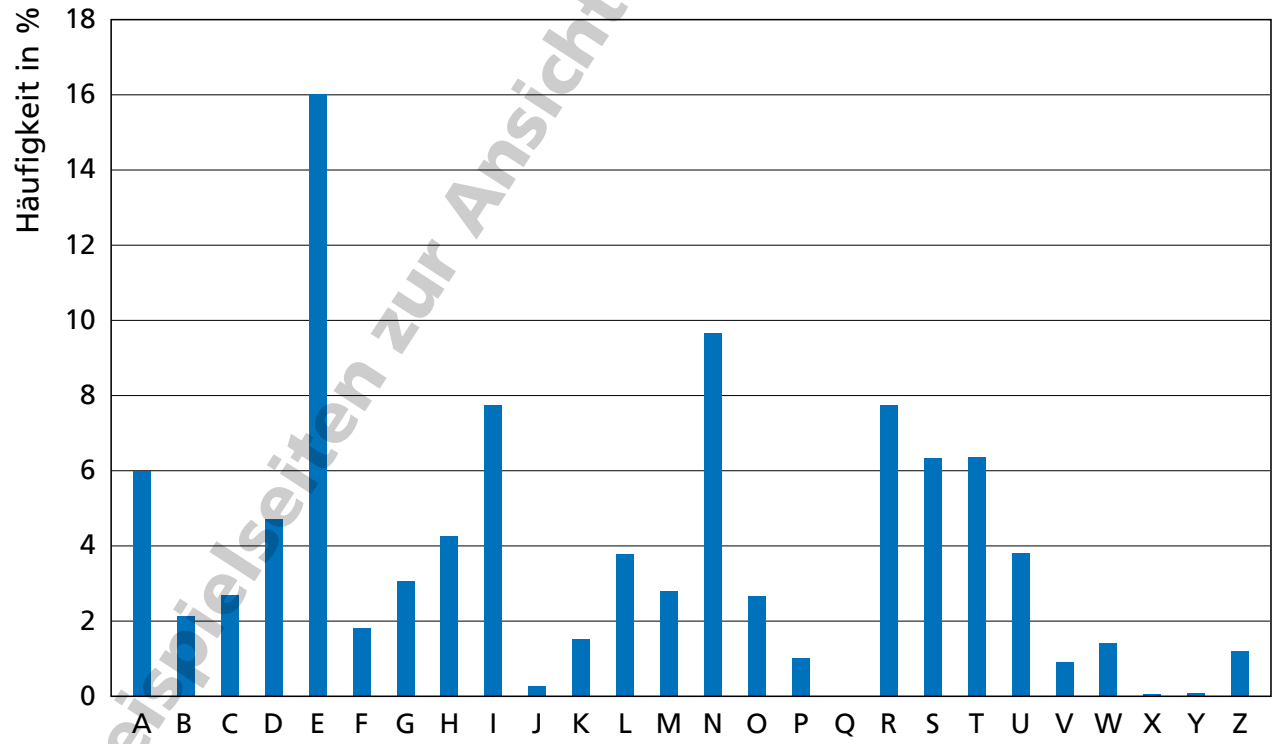
Wenn man die Sprache des Geheimtextes kennt, kann man die Häufigkeitsverteilung dann mit der eines Vergleichstextes oder einer wissenschaftlichen Statistik wie der des Instituts für Deutsche Sprache vergleichen.

Der häufigste Buchstabe oder das häufigste Symbol eines deutschen Geheimtextes steht für das Klartext-E, der zweithäufigste für das N usw.

Ist der Text mit einer einfachen Caesar-Verschlüsselung verschlüsselt, reichen diese beiden Buchstaben aus, um den Schlüssel zu ermitteln und damit den kompletten Text zu entschlüsseln.

Ist der Text mit einer Caesar-Verschlüsselung mit Schlüsselwort verschlüsselt, beginnt man nach dem Ermitteln der Buchstaben E und N zu kombinieren und kurze oder wahrscheinliche Wörter zu erraten. So gewinnt man Buchstabe für Buchstabe hinzu, bis die gesamte Verschlüsselung gebrochen und der Geheimtext entziffert ist.

Häufigkeitsverteilung der Buchstaben in der deutschen Sprache



Häufigkeitsverteilung der Buchstaben in der deutschen Sprache, ermittelt vom Leibniz-Institut für Deutsche Sprache (IDS) in Mannheim aus einer Textsammlung mit insgesamt fast 150 Milliarden Zeichen. (http://www1.ids-mannheim.de/kl/projekte/methoden/derewo.html#derechar (Stand Oktober 2019))

Häufigkeitsanalyse

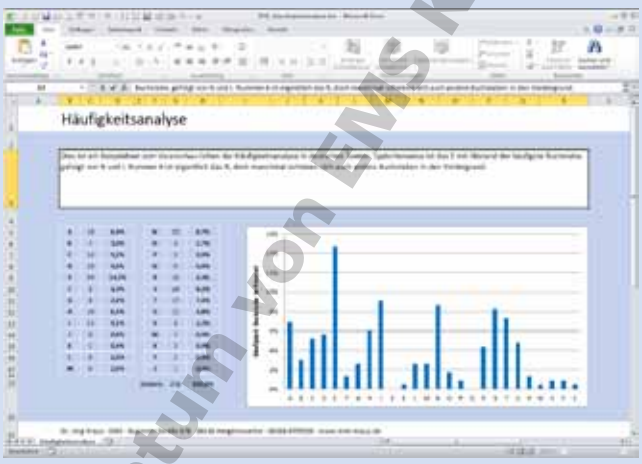
Aufgabe 1

Wähle einen kurzen deutschen Text von 100 bis 200 Zeichen Länge aus und ermittle die Häufigkeitsverteilung der Buchstaben in diesem Text. Welche Buchstaben kommen am häufigsten vor?

Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

Beispieltext_Haeufigkeitsanalyse_1.txt:
Dies ist ein Beispieltext zum Veranschaulichen der Häufigkeitsanalyse in deutschen Texten. Typischerweise ist das E mit Abstand der häufigste Buchstabe, gefolgt von N und I. Nummer 4 ist eigentlich das R, doch manchmal schieben sich auch andere Buchstaben in den Vordergrund.

Häufigste Buchstaben: E, N, I



Aufgabe 2

Der folgende deutsche Text wurde mit der Caesar-Verschlüsselung verschlüsselt. (Text_Haeufigkeitsanalyse_2.txt)

KLY HYHIPZJOL NLSLOYAL HS RPUKP ZAHTTAL HBZ LPULY DVOSOHILUKLU BUK LPUMSBZZYLPJOLU HYHIPZJOLU MHTPSPL HBZ KLY YLNPVU ZBLKSPJO CVU IHNKHK TPA OPSML CVU BLILYZLAGLYU BLILYAYBN LY LPULU NYVZZALPS KLZ DLYRZ CVU HYPZAVALSLZ BUK WSHAVU PUZ HYHIPZJOL KH LY HBJO LPNLUL WOPSVZVWOPZJOL ZJOYPMALU CLYMHZZAL DPYK LY HBJO HSZ LYZALY WOPSVZVWO KLY HYHIPZJOLU DLSA ILGLPJOULA ULILU KLY WOPSVZVWOPL ILMHZZAL ZPJO HS RPUKP HBJO TPA WOFZPR HZAYVUVTPL TLKPGPU BUK RBUZA PU ZLPULU ZJOYPMALU GBY HSJOLTPL ILGDLPMLSAL LY KHZZ ZPJO NVSK BUK ZPSILY HBZ DLUPNLY DLYACVSSLU TLAHSSLU OLYZALSSLU SHZZLU

a) Ermittle die Häufigkeitsverteilung der Buchstaben im verschlüsselten Text. Welcher Buchstabe kommt am häufigsten vor? Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

Der Buchstabe L kommt am häufigsten vor.

Häufigkeitsanalyse

b) Welcher Schlüssel wurde beim Verschlüsseln mit Hilfe der Caesar-Verschlüsselung vermutlich eingesetzt? Begründe deine Vermutung.

Da in deutschen Texten E der häufigste Buchstabe ist, könnte das L für das E stehen. Damit aus dem E ein L wird, muss mit dem Schlüssel 7 verschlüsselt werden.

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	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

c) Überprüfe deine Vermutung, indem du den Text mit dem Gegenstück zu diesem Schlüssel entschlüsselst.

Zum Entschlüssel muss der Schlüssel 19 verwendet werden, da 26 – 7 = 19 ist.

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
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

DER ARABISCHE GELEHRTE AL KINDI STAMMTE AUS EINER WOHLHABENDEN UND EINFLUSSREICHEN ARABISCHEN FAMILIE AUS DER REGION SUEDLICH VON BAGDAD MIT HILFE VON UEBERSETZERN UEBERTRUG ER EINEN GROSSTEIL DES WERKS VON ARISTOTELES UND PLATON INS ARABISCHE DA ER AUCH EIGENE PHILOSOPHISCHE SCHRIFTEN VERFASSTE WIRD ER AUCH ALS ERSTER PHILOSOPH DER ARABISCHEN WELT BEZEICHNET NEBEN DER PHILOSOPHIE BEFASSTE SICH AL KINDI AUCH MIT PHYSIK ASTRONOMIE MEDZIN UND KUNST IN SEINEN SCHRIFTEN ZUR ALCHEMIE BEZWEIFELTE ER DASS SICH GOLD UND SILBER AUS WENIGER WERTVOLLEN METALLEN HERSTELLEN LASSEN

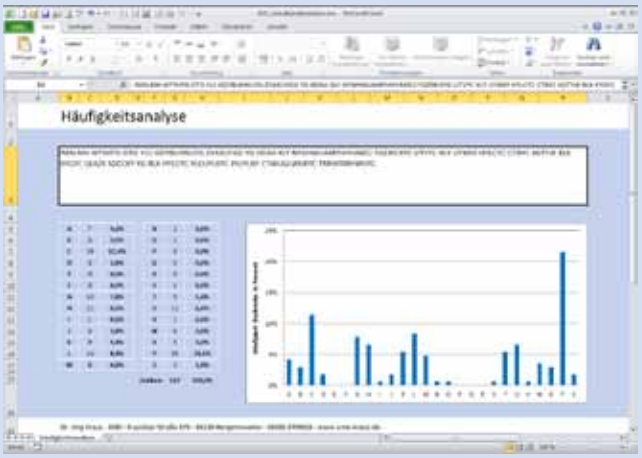
Aufgabe 3

Der folgende Text wurde mit der Caesar-Verschlüsselung mit Schlüsselwort verschlüsselt. (Text_Haeufigkeitsanalyse_3.txt)

IMALMH WTYHTG OTG YLC GDYBLHWUYG ZYAXUYGG YG HDAA XLY NYGHWUAMYHHYAMCJ YGZMCXYC UTVYC XLY UYMKY HYLCYC CTBYC KGTYJK BLK XYGYC ULAZY SDCCKY YG BLK HYLCYC YLCUYLKYC JYUYLBY CTWUGLWUKYC TMHKTMHWUYC

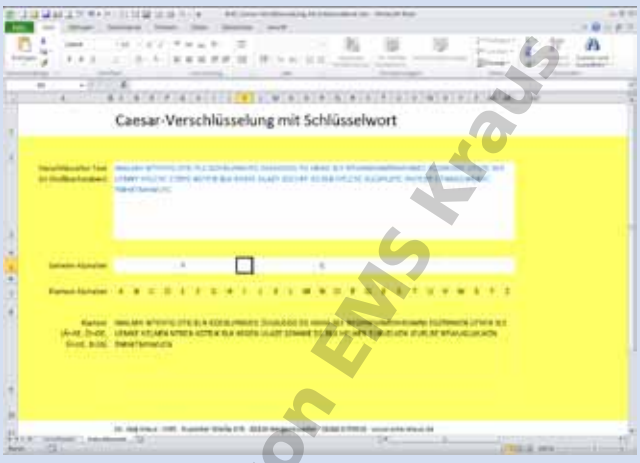
a) Ermittle die Häufigkeitsverteilung der Buchstaben im verschlüsselten Text. Welche beiden Buchstaben kommen am häufigsten vor? Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

Die Buchstaben Y und C kommen am häufigsten vor.



Häufigkeitsanalyse

b) Für welche Klartextbuchstaben stehen diese beiden Buchstaben vermutlich?
Ersetze diese ersten beiden Buchstaben in dem verschlüsselten Text.
Nutze dafür z. B. die Datei EMS_Caesar-Verschluesselung_mit-Schluesselwort.xlsx (Blatt Entschlüsseln)



Da in deutschen Texten E und N die häufigsten Buchstaben sind, könnten das Y für das E und das C für das N stehen.

c) Brich nun die Verschlüsselung, indem du die restlichen Buchstaben des Geheimalphabets ermittelst. Beginne mit kurzen Wörtern und erinnere dich daran, wie das Geheimalphabet links und rechts vom Schlüsselwort aufgebaut ist.

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

d) Wie lautet das Schlüsselwort und auf welcher Position steht es?

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

Das Schlüsselwort lautet JULIUS auf G.

e) Notiere den entschlüsselten Text.

JULIUS CAESAR WAR EIN ROEMISCHER FELDHERR
ER SOLL DIE VERSCHLUESSELUNG ERFUNDEN HABEN
DIE HEUTE SEINEN NAMEN TRAEGT
MIT DEREN HILFE KONNTE ER MIT SEINEN EINHEITEN
GEHEIME NACHRICHTEN AUSTAUSCHEN

Sicherheitsaspekte bei mobilen Geräten

Smartphones sind aus unserem Alltag nicht mehr wegzudenken. Mehr als fünf Stunden täglich sind Jugendliche mit ihrem Smartphone im Internet, so ein Ergebnis der Postbank Jugend-Digitalstudie 2019 [1]. Zugleich sind Smartphones bei Dieben begehrt. Um die 600 Geräte werden in Deutschland täglich gestohlen [2]. Grund genug, das eigene Smartphone nie aus den Augen zu lassen und sich Gedanken über die Sicherheit von Smartphones und anderen mobilen Datenträgern zu machen.

Bildschirmsperre

Die Bildschirmsperre gehört zu den Basisschutzmaßnahmen. Je nach Gerät kann sie auf unterschiedliche Weise entsperrt werden:

Eine häufig genutzte Technik ist das **Wischmuster**. Ein sicheres Wischmuster sollte keiner einfachen geometrischen Figur entsprechen, nicht in den Ecken starten und nicht nur direkte Verbindungen zwischen Punkten nutzen. Zusätzlich sollte das Display regelmäßig gesäubert werden, damit die fettigen Wischspuren den Code nicht ganz einfach verraten.

Ähnlich häufig wird ein vierstelliger **PIN-Code** zum Entsperren des Bildschirms genutzt. Mathematisch sind bei 4-stelligen PIN-Codes 10 000 Varianten möglich. Doch auch bei diesem Verfahren bevorzugen viele Nutzer sehr einfache Codes, um ihr Smartphone zu schützen.

PIN-Code	Nutzer
1234	10,713 %
1111	6,016 %
0000	1,881 %
1212	1,197 %
7777	0,745 %

Eine Analyse von 3,4 Mio. PIN-Codes ergab, dass ein Fünftel der Nutzer einen dieser fünf einfachen PIN-Codes verwendet. [3]

Neben der Verwendung von Wischmuster und PIN-Codes gibt es je nach Gerät weitere Verfahren zum Sperren des Bildschirms, die sicherer sind:

- Passwort
- Gesichtserkennung
- Fingerabdruck

Vorsichtsmaßnahmen

Neben dem Nutzen einer Bildschirmsperre gibt es einige Vorsichtsmaßnahmen, durch die sich mobile Geräte schützen lassen [4]:

- vorhandene Sicherheitsfunktionen des Smartphones einschalten, Sicherheitsupdates direkt nach dem Erscheinen einspielen
- Apps nur aus vertrauenswürdigen Quellen installieren, Zugriffsrechte der Apps auf die zum Erfüllen der Funktion notwendigen begrenzen
- Drahtlosschnittstellen wie WLAN oder Bluetooth und die GPS-Funktion deaktivieren, wenn sie nicht benötigt werden
- öffentliche Hotspots und WLAN-Netze mit erhöhter Vorsicht nutzen
- Funktionen zur Datenverschlüsselung nutzen, auch für Daten auf einer zusätzlichen SD-Karte
- Daten von mobilen Geräten regelmäßig auf einem Backup-Medium sichern
- mobile Geräte auch über USB nur an vertrauenswürdige Rechner anschließen

Wenn das Smartphone weg ist

Wenn das Smartphone verloren oder gestohlen ist, kann es mit Hilfe geeigneter Apps aus der Ferne gesperrt werden. Dadurch werden die persönlichen Daten auf dem Smartphone gelöscht oder sind nicht mehr aufzurufen.

Nach dem Sperren des Smartphones sollte auch die SIM-Karte beim Mobilfunkanbieter gesperrt werden. Dafür braucht man diese Angaben:

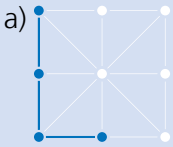
- Rufnummer deines Smartphones
- SIM-Kartennummer
- Kundennummer

Möchte man das Smartphone bei der Polizei als gestohlen melden, benötigt man die IMEI-Nummer des Geräts. Die IMEI-Nummer ist eine 15-stellige Nummer, über die jedes Smartphone identifiziert werden kann. Die IMEI-Nummer des eigenen Smartphones wird angezeigt, wenn man *#06# (Stern-Raute-null-sechs-Raute) ins Handy-Display eintippt, als wenn man telefonieren will.

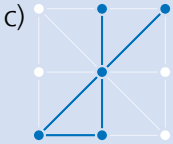
[1] Postbank Jugend-Digitalstudie 2019, https://www.presseportal.de/pm/6586/4395099 (Stand Oktober 2019)
[2] https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/handy-geklaut-sperrung-oberstes-gebot-13870 (Stand Oktober 2019)
[3] http://www.datagenetics.com/blog/september32012/ (Stand Oktober 2019)
[4] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html;jsessionid=EA13DDE2558C53F9760DB37D5AC31BE5.2_cid369 (Stand Oktober 2019)

Sicherheitsaspekte bei mobilen Geräten

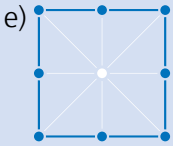
Aufgabe 1
Bewerte die Sicherheit der folgenden Wischmuster mit „sicher“ oder „unsicher“.

a)  unsicher

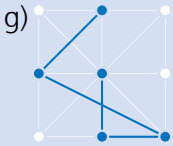
b)  unsicher

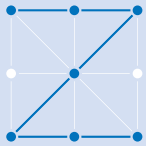
c)  sicher

d)  sicher

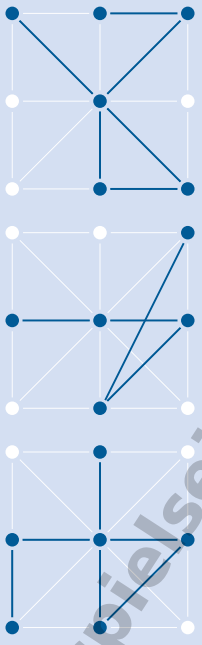
e)  unsicher

f)  sicher

g)  sicher

h)  unsicher

Aufgabe 2
Zeichne drei sichere Wischmuster.

z. B. 

Aufgabe 3
a) Notiere drei 4-stellige PIN-Codes, die du als unsicher ansiehst.

z. B. 5555, 2424, 4321

b) Notiere drei 4-stellige PIN-Codes, die du als sicher ansiehst.

z. B. 7053, 9260, 5836

Aufgabe 4
a) Erkläre, warum es besonders viele PIN-Codes gibt, die mit den Ziffern 19 beginnen.

Viele Nutzer von Smartphones verwenden ihr Geburtsjahr als PIN-Code.

b) Erkläre, warum es vor allem in englischsprachigen Ländern besonders viele PIN-Codes gibt, die mit Null beginnen.

Viele Nutzer von Smartphones verwenden ihr Geburtsdatum als PIN-Code. Im Englischen wird im Datum der Monat vor dem Tag geschrieben. Die PIN-Codes für alle Geburtstage von Januar bis September, also drei Viertel dieser PIN-Codes, beginnen mit Null.

Aufgabe 5
Erstelle eine Notfallkarte für dein Smartphone, auf der du alle Angaben notierst, die du beim Verlust des Gerätes benötigst:
- Rufnummer deines Smartphones
- Marke und Typ
- IMEI-Nummer (*#06#)
- SIM-Kartennummer
- Mobilfunkanbieter
- Kundennummer
- Telefonnummer für Sperrung der SIM-Karte