Themen

weitere Themen siehe Seite 7

Themen

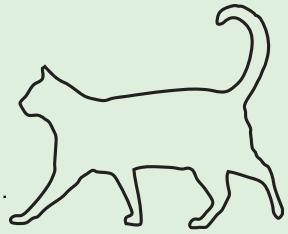
weitere Themen siehe Seite 9

Themen

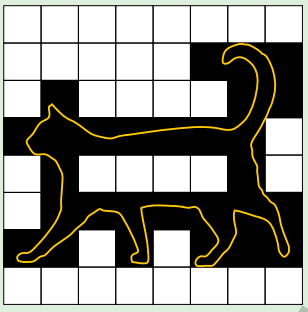
Codierung Pixel-Grafiken

Digitale Bilder bestehen aus unzähligen kleinen Kästchen, die auch Pixel genannt werden. Sie sind so klein, dass wir sie normalerweise gar nicht wahrnehmen. Nur wenn man ein Foto sehr stark vergrößert, kann man die unterschiedlich gefärbten Kästchen sehen.

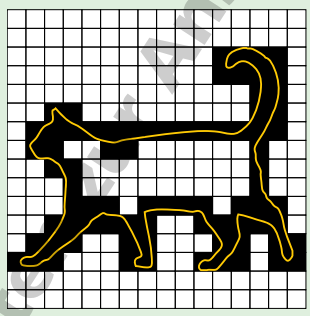
Foto: Joshua Willson (Pixabay)



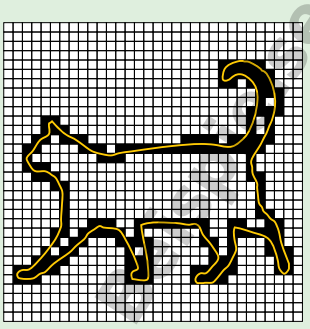
Das Prinzip, nach dem digitale Bilder aufgebaut sind, lässt sich am besten anhand einer schwarz-weißen-Zeichnung erklären. Über die Zeichnung wird – bildlich gesprochen – ein Kästchenraster gelegt. Alle Kästchen, durch die Linien der Zeichnung hindurchführen, werden schwarz gefärbt. Je feiner das Raster ist, desto näher ist das Ergebnis an der ursprünglichen Zeichnung.



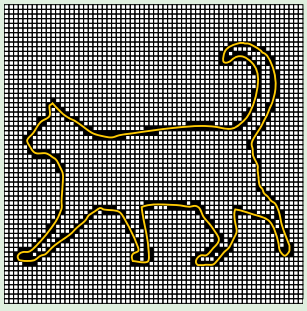
8 × 8 Pixel



16 × 16 Pixel



32 × 32 Pixel



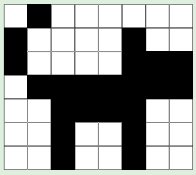
64 × 64 Pixel

Die Farben der einzelnen Kästchen in unserem Beispiel können nur zwei Werte annehmen: schwarz und weiß. Es bietet sich daher an, die weißen Kästchen mit einer Null und die schwarzen Kästchen mit einer Eins zu codieren.

Für die Übertragung von solch einfachen schwarz-weißen Bilder wurde in den 1980er Jahren das PBM-Format entwickelt. PBM steht für Portable Bitmap. PBM-Dateien kann man wie einen Text in einem Editor schreiben.

Das folgende Beispiel zeigt das Prinzip:
PBM-Dateien beginnen stets mit dem Kürzel P1. Die Ziffern 8 und 7 geben die Breite und Höhe des Bildes an. Danach folgen Nullen und Einsen, die in einer fortlaufenden Schlange für weiße und schwarze Pixel stehen.

```
P1
8 7
0 1 0 0 0 0 0 0 1 0 0 0 0 1 0 0 1
0 0 0 0 1 1 1 0 1 1 1 1 1 1 1 0 0
1 1 1 1 0 0 0 0 1 0 0 1 0 0 0 0 1
0 0 1 0 0
```

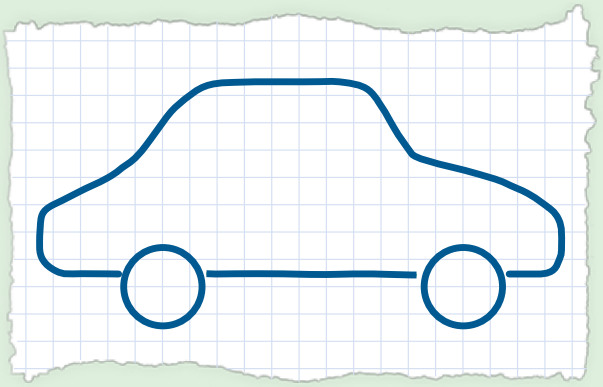


Speichert man diesen Beispieltext mit der Dateiendung .pbm ab, kann man die Datei anschließend in einem Bildbetrachtungsprogramm wie beispielsweise IrfanView, Gimp oder Photoshop öffnen.

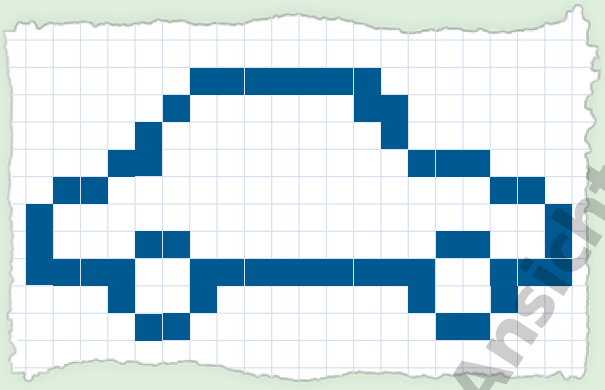
Hinweis zu IrfanView: Damit nach dem Vergrößern des Bildes die einzelnen Pixel zu erkennen sind, muss man im Menüpunkt „View“ unter „Display Options“ die Option „Use resample for zooming“ ausschalten.

Codierung Pixel-Grafiken

Aufgabe 1
Fertige eine kleine Zeichnung aus einfachen Linien auf Kästchenpapier an.



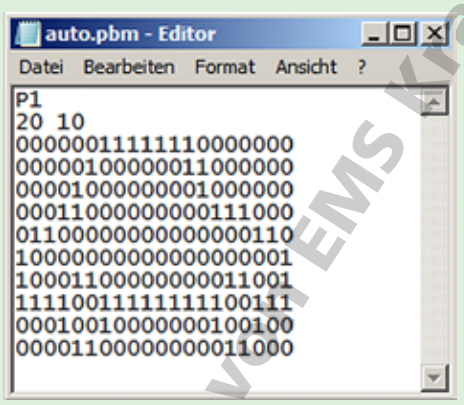
Aufgabe 2
Male alle Kästchen schwarz aus, durch die Linien deiner Zeichnung hindurchführen.



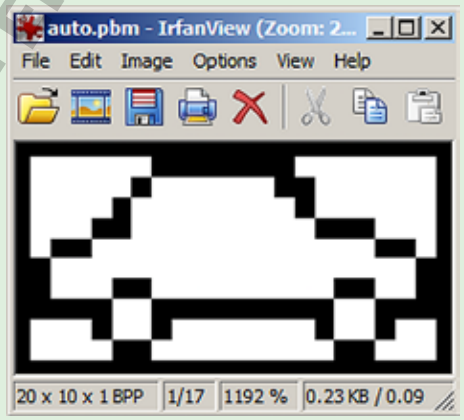
Aufgabe 3
Schreibe für deine Kästchenfolge eine Textdatei aus Einsen und Nullen.

```
0000001111111000000
0000010000001100000
0001000000000100000
0001100000000011000
0110000000000000110
1000000000000000001
1000110000000011001
1111001111111100111
0001001000000010010
0000110000000011000
```

Aufgabe 4
Stelle die Angaben für Breite und Höhe sowie das Kürzel für das PBM-Format voran und speichere die Datei ab.



Aufgabe 5
Öffne die Datei in einem Bildbetrachtungsprogramm (z. B. IrfanView) und überprüfe, ob das Resultat deiner Zeichnung entspricht.



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.

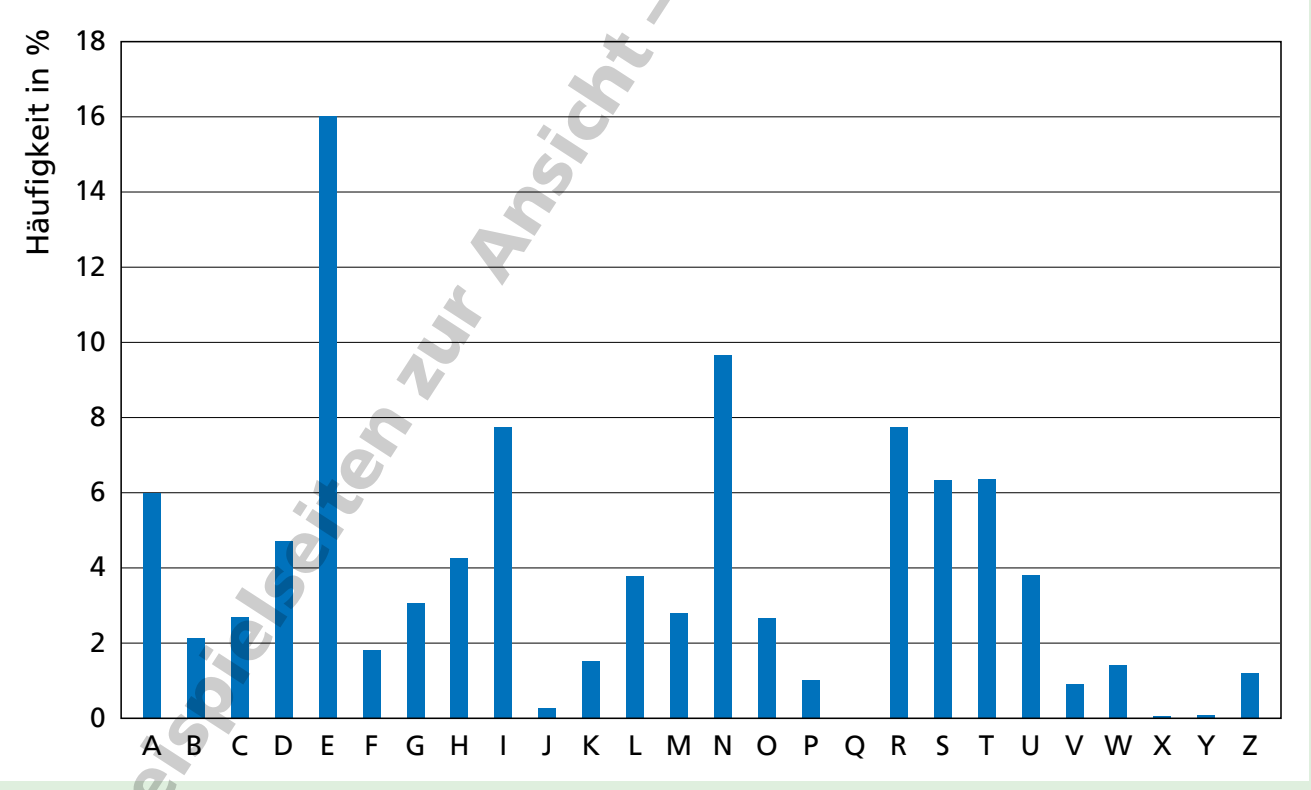
Wenn man die Sprache des Geheimtextes kennt, kann man die Häufigkeitsverteilung dann mit der eines Vergleichstextes oder einer wissenschaftlichen Statistik wie der des Instituts für Deutsche Sprache vergleichen.

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

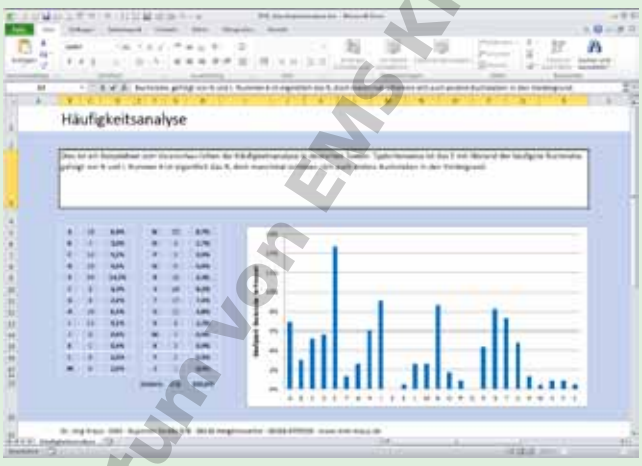
Aufgabe 1

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



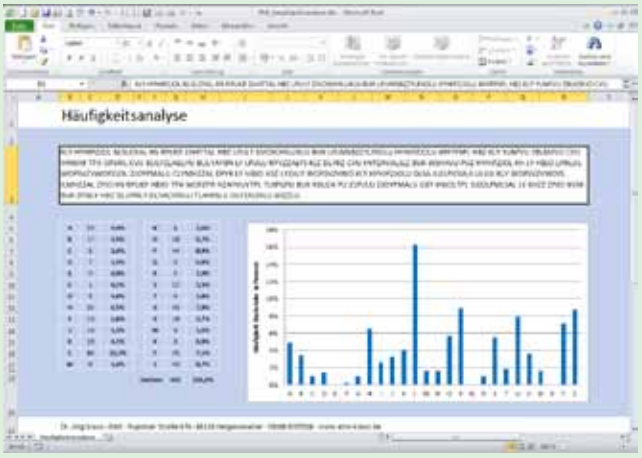
Aufgabe 2

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

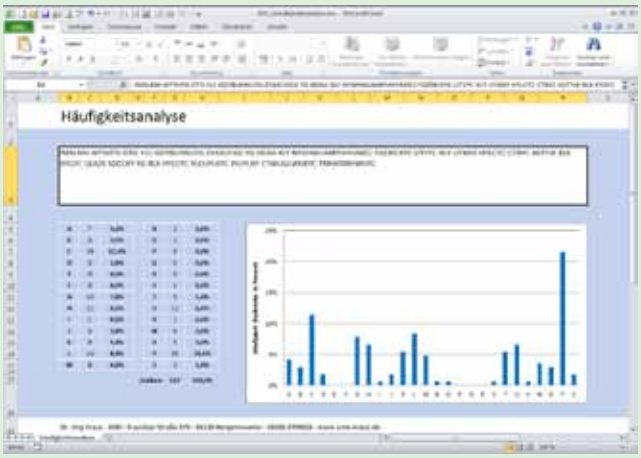
Aufgabe 3

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

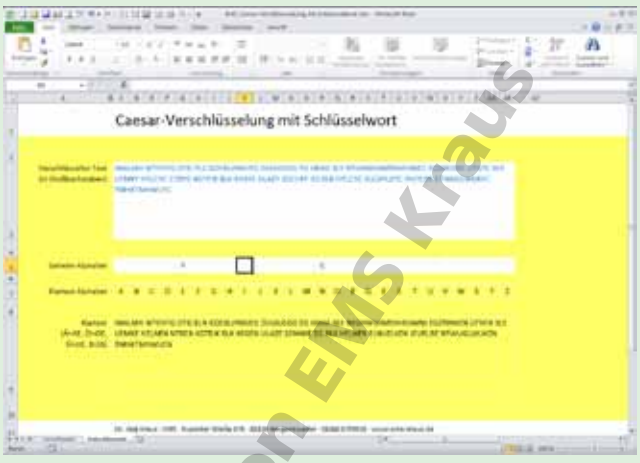
a) Ermittle die Häufigkeitsverteilung der Buchstaben im verschlüsselten Text. Welche beiden Buchstaben kommen am häufigsten vor? Nutze dafür z. B. die Datei EMS_Haeufigkeitsanalyse.xlsx.

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:

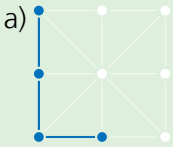
- Rufnummer deines Smartphones
- SIM-Kartennummer
- Kundennummer

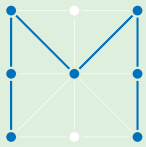
Möchte man das Smartphone bei der Polizei als gestohlen melden, benötigt man die IMEI-Nummer des Geräts. Die IMEI-Nummer ist eine 15-stellige Nummer, über die jedes Smartphone identifiziert werden kann. Die IMEI-Nummer des eigenen Smartphones wird angezeigt, wenn man *#06# (Stern-Raute-null-sechs-Raute)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

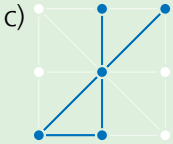
[1] Postbank Jugend-Digitalstudie 2019, https://www.presseportal.de/pm/6586/4395099 (Stand Oktober 2019)
[2] https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/handy-geklaut-sperrung-oberstes-gebot-13870 (Stand Oktober 2019)
[3] http://www.datagenetics.com/blog/september32012/ (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

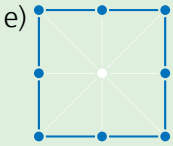
Aufgabe 1
Bewerte die Sicherheit der folgenden Wischmuster mit „sicher“ oder „unsicher“.

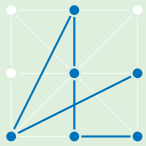
a)  unsicher

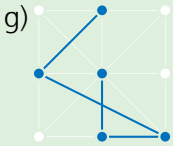
b)  unsicher

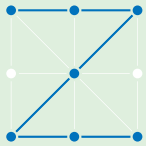
c)  sicher

d)  sicher

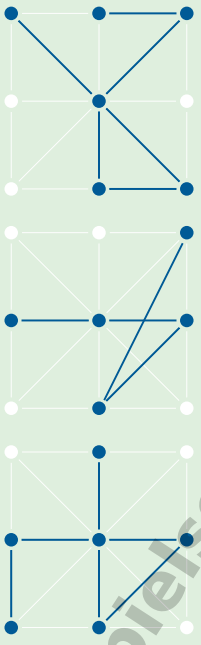
e)  unsicher

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

Vigenère-Verschlüsselung

Die Vigenère-Verschlüsselung stammt aus dem 16. Jahrhundert und ist nach dem französischen Diplomaten Blaise de Vigenère (1523 – 1596) benannt. Im Gegensatz zur Caesar-Verschlüsselung, bei der die Buchstaben des Klartextes durch Buchstaben eines einzigen Alphabets ersetzt werden, arbeitet man dabei mit 26 Alphabeten. Das Verfahren gehört daher zu den polyalphabetischen Substitutionsverfahren (von lateinisch substituere = „ersetzen“).

Die 26 Alphabete werden – jeweils um eine Stelle verschoben – im Vigenère-Quadrat angeordnet. Welches Alphabet für das Verschlüsseln eines Buchstabens verwendet wird, legt der Schlüssel fest, den Sender und Empfänger der Botschaft kennen müssen.

Beim Verschlüsseln wird das Schlüsselwort (STORCH) über dem Klartext notiert. Der Schlüsselbuchstabe **S** wird in der linken Spalte gesucht. Der Klartextbuchstabe **I** wird in der Zeile oben gesucht. Der Geheimtextbuchstabe A findet sich am Kreuzungspunkt der Spalte **I** mit der Zeile **S**.

Schlüssel	**S**	**T**	**O**	**R**	**C**	**H**	**S**	**T**	**O**	**R**
Klartext	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**
Geheimtext	A	G	T	F	T	T	S	M	W	B

Beim Entschlüsseln wird der Schlüsselbuchstabe **H** in der linken Spalte gesucht. In der **H**-Zeile sucht man nach dem Geheimtext-Buchstaben T. In der betreffenden Spalte findet sich oben der Klartextbuchstabe **M**.

Schlüssel	**S**	**T**	**O**	**R**	**C**	**H**	**S**	**T**	**O**	**R**
Geheimtext	A	G	T	F	T	T	S	M	W	B
Klartext	**I**	**N**	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**K**

Die Vigenère-Verschlüsselung ist deutlich sicherer als die Caesar-Verschlüsselung. Durch das Verschlüsseln gleicher Buchstaben mit unterschiedlichen Schlüsselbuchstaben kann sie nicht durch eine Häufigkeitsanalyse geknackt werden. Für einen Brute-Force-Angriff ist die Anzahl möglicher Schlüssel zu groß.

Dennoch gelang es dem englischen Wissenschaftler Charles Babbage (1791 – 1871) im Jahr 1854 mit dem Vigenère-Verfahren verschlüsselte Texte zu entziffern.

Schlüssel \ 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
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

Vigenère-Verschlüsselung

Aufgabe 1
Verschlüssele diese Orte mit dem Schlüsselwort ROM.

MAILAND
BOLOGNA
TURIN
PALERMO
NEAPEL
VERONA

Schlüssel	R	O	M	R	O	M	R
Klartext	**M**	**A**	**I**	**L**	**A**	**N**	**D**
Geheimtext	D	O	U	C	O	Z	U

Schlüssel	R	O	M	R	O	M	R
Klartext	**B**	**O**	**L**	**O**	**G**	**N**	**A**
Geheimtext	S	C	X	F	U	Z	R

Schlüssel	R	O	M	R	O
Klartext	**T**	**U**	**R**	**I**	**N**
Geheimtext	K	I	D	Z	B

Schlüssel	R	O	M	R	O	M	R
Klartext	**P**	**A**	**L**	**E**	**R**	**M**	**O**
Geheimtext	G	O	X	V	F	Y	F

Schlüssel	R	O	M	R	O	M
Klartext	**N**	**E**	**A**	**P**	**E**	**L**
Geheimtext	E	S	M	G	S	X

Schlüssel	R	O	M	R	O	M
Klartext	**V**	**E**	**R**	**O**	**N**	**A**
Geheimtext	M	S	D	F	B	M

MAILAND DOUCOZU
BOLOGNA SCXFUZR
TURIN KIDZB
PALERMO GOXVFYF
NEAPEL ESMGSX
VERONA MSDFBM

Aufgabe 2
Welche Alpenberge sind hier verschlüsselt? (Schlüsselwort: GIPFEL)

FCVXTTZHT
SIIYICNWGS
CIIEQLTV
PCCLJCGC
CQAIWAOBOJ
TMQJPSUZC

Schlüssel	G	I	P	F	E	L	G	I	P
Geheimtext	F	C	V	X	T	T	Z	H	T
Klartext	**Z**	**U**	**G**	**S**	**P**	**I**	**T**	**Z**	**E**

Schlüssel	G	I	P	F	E	L	G	I	P	F
Geheimtext	S	I	I	Y	I	C	N	W	G	S
Klartext	**M**	**A**	**T**	**T**	**E**	**R**	**H**	**O**	**R**	**N**

Schlüssel	G	I	P	F	E	L	G	I
Geheimtext	C	I	I	E	Q	L	T	V
Klartext	**W**	**A**	**T**	**Z**	**M**	**A**	**N**	**N**

Schlüssel	G	I	P	F	E	L	G	I
Geheimtext	P	C	C	L	J	C	G	C
Klartext	**J**	**U**	**N**	**G**	**F**	**R**	**A**	**U**

Schlüssel	G	I	P	F	E	L	G	I	P	F
Geheimtext	C	Q	A	I	W	A	O	B	O	J
Klartext	**W**	**I**	**L**	**D**	**S**	**P**	**I**	**T**	**Z**	**E**

Schlüssel	G	I	P	F	E	L	G	I	P
Geheimtext	T	M	Q	J	P	S	U	Z	C
Klartext	**N**	**E**	**B**	**E**	**L**	**H**	**O**	**R**	**N**

FCVXTTZHT ZUGSPITZE
SIIYICNWGS MATTERHORN
CIIEQLTV WATZMANN
PCCLJCGC JUNGFRAU
CQAIWAOBOJ WILDSPITZE
TMQJPSUZC NEBELHORN

Vigenère-Verschlüsselung

Aufgabe 3

Verschlüssele dieses Zitat, das dem Schriftsteller Mark Twain (1835 – 1910) zugeschrieben wird:
„Das Geheimnis des Vorankommens ist das Anfangen."

Verwende das Schlüsselwort GEHEIM.

DASGE HEIMN ISDES VORAN KOMME NSIST DASAN FANGE N

JEZKM TKMTR QEJIZ ZWDGR RSUYK RZMAF JEZ EV RGRNI V

Aufgabe 4

Entschlüssele die Aussage von Napoléon Bonaparte (1769 – 1821) über das Wetter in Deutschland.

Verwende das Schlüsselwort FRANKREICH.

IZEQO LXAEO JEHNL VRAGJ MJMBX RXMYP SKEEE EHAGJ MJMBX RXMML NEEAC FQUGY

DIEDE UTSCH ENHAB ENSEC HSMON ATEWI NTERU
NDSEC HSMON ATEKE INENS OMMER

„Die Deutschen haben sechs Monate Winter und sechs Monate keinen Sommer."

Schlüssel	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
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	

Zeichenvorrat, Codewörter

Codes werden verwendet, um eine Information für einen Anwendungsfall optimal darzustellen.

Dabei muss man zwei Varianten von Codes unterscheiden:

- Alphabete für besondere Anwendungen.
  Sie benötigen einen großen Zeichenvorrat, um Informationen möglichst detailliert darstellen zu können.
- Codes zur Darstellung umfangreicher Informationen auf kleinen Flächen.
  Sie lassen aufgrund der begrenzten Zeichenzahl nur eine bestimmte Anzahl unterschiedlicher Codewörter zu.

Die **Brailleschrift** ist ein Beispiel für ein spezielles Alphabet. Sie ermöglicht es Blinden, Texte und sogar ganze Bücher zu lesen. Die Zeichen der Brailleschrift bestanden ursprünglich aus sechs Punkten, die mit ihren beiden Möglichkeiten (flach/erhaben) einen Zeichenvorrat von 2^6 (also 64) Zeichen ergeben.

a, 1 b, 2 c, 3

Dieser Zeichenvorrat erwies sich bald als zu klein. Deshalb wurde in den 1980er Jahren das 8-Punkt-Computerbraille entwickelt. Die 8 Punkte ergeben einen Vorrat von 2^8 (also 256) Zeichen. Neben den 64 Zeichen der ursprünglichen Brailleschrift standen damit weitere 192 Zeichen zur Verfügung, die nun auch Groß- und Kleinschreibung und Zahlen ohne vorangestellte Hilfszeichen ermöglichten.

Der ursprüngliche **ASCII-Code** bestand aus 7 Bit. Er erlaubte die Darstellung von $2^7 = 128$ Zeichen. Zahlreiche Zeichen wie die deutschen ß oder ä, die im Englischen nicht vorkommen, waren mit dem ASCII-Code nicht darstellbar. Der ANSI-Code – eine Erweiterung des ASCII-Codes – besteht aus 8 Bit. Mit ihm lassen sich $2^8 = 256$ Zeichen, also auch zahlreiche Sonderzeichen, darstellen.

Seit 1991 gibt es den auf Basis des ASCII-Codes entwickelten Unicode-Standard, einen 16-Bit-Code, der neben den europäischen Zeichen auch kyrillische, indische, chinesische und japanische Schriftzeichen enthält. Insgesamt können mit dem Unicode $2^{16} = 65\,536$ Zeichen codiert werden.

Das **Kfz-Kennzeichen** ist ein Beispiel für einen Code, mit dessen Hilfe Informationen auf einer begrenzten Fläche dargestellt werden.
Links von TÜV-Plakette und Zulassungsplakette ist der Landkreis bzw. die kreisfreie Stadt codiert, in der das Fahrzeug zugelassen ist. Dafür stehen maximal 3 Zeichen zur Verfügung.

Danach folgen ein oder zwei Buchstaben und maximal vier Ziffern. Diese Buchstaben und Ziffern sind entscheidend dafür, wie viele unterschiedliche Kennzeichen (Codewörter) in einem Landkreis bzw. in einer kreisfreien Stadt möglich sind.

Unter der Voraussetzung, dass alle Kombinationen von Buchstaben und Ziffern (außer 0, 00 usw.) vergeben werden, lässt sich maximale Anzahl pro Landkreis ermitteln.

Für Kennzeichen mit einem Buchstaben und zwei Ziffern wie in unserem Beispiel gibt es
26 Buchstaben × 99 Zahlen = 2 574 Möglichkeiten.

Zeichenvorrat, Codewörter

Aufgabe 1
Der französische Offizier Charles Barbier de la Serre (1767 – 1841) entwickelte die so genannte Nachtschrift, einen Vorläufer der Brailleschrift. Die Zeichen der Schrift bestanden aus jeweils 12 erhabenen Punkten, die ertastet werden konnten.

Wie viele Zeichen konnten mit dieser Schrift codiert werden?

Der Code hat 12 Punkte mit jeweils 2 Möglichkeiten (flach oder erhaben).

Daraus resultieren $2^{12} = 4\,096$ Zeichen.

Aufgabe 2
Der Baudot-Code ist ein 5-Bit-Zeichencode, der 1870 von Jean-Maurice-Émile Baudot (1845 – 1903) für ein von ihm entwickeltes Telegrafengerät erfunden wurde. Jedes Bit kann den Wert 1 oder 0 haben.

a) Wie viele Zeichen konnten mit dem Baudot-Code codiert werden?

b) Reicht der Code für die 26 Buchstaben des Alphabets und die zehn Ziffern aus?

a) Der Code hat 5 Punkte mit jeweils 2 Möglichkeiten (1 oder 0).

Daraus resultieren $2^5 = 32$ Zeichen.

b) Die Zeichenzahl reicht nicht aus, um alle 26 Buchstaben des Alphabets und 10 Ziffern darzustellen.

Aufgabe 3
Im Zulassungsbezirk Berlin waren zum 1. Januar 2019 1 524 484 Fahrzeuge und Fahrzeuganhänger zugelassen.[1)]
Wie viele weitere Fahrzeuge könnten in Berlin noch zugelassen werden, bevor der Berliner Zulassungsbehörde die Kennzeichen ausgehen?

Kennzeichen mit einem Buchstaben und maximal vier Ziffern erlauben

26 Buchstaben x 9 999 Zahlen
= 259 974 unterschiedliche Kennzeichen.

Kennzeichen mit zwei Buchstaben und maximal vier Ziffern erlauben

26 x 26 Buchstaben x 9 999 Zahlen
= 6 759 324 unterschiedliche Kennzeichen.

Es könnten noch 5 494 814 weitere Fahrzeuge und Fahrzeuganhänger zugelassen werden.

Aufgabe 4
Die kreisfreie Stadt Suhl in Thüringen ist der Zulassungsbezirk in Deutschland mit der kleinsten Anzahl zugelassener Fahrzeuge.
Zum 1. Januar 2019 waren dort 26 922 Kraftfahrzeuge und Fahrzeuganhänger zugelassen.[1)]

Würde die mögliche Anzahl an Kennzeichen für den Fahrzeugbestand ausreichen, wenn die Zulassungsstelle in Suhl nur Kennzeichen mit einem Buchstaben und maximal 3 Ziffern ausgeben würde?

Kennzeichen mit einem Buchstaben und maximal drei Ziffern erlauben

26 Buchstaben x 999 Zahlen
= 25 974 unterschiedliche Kennzeichen.

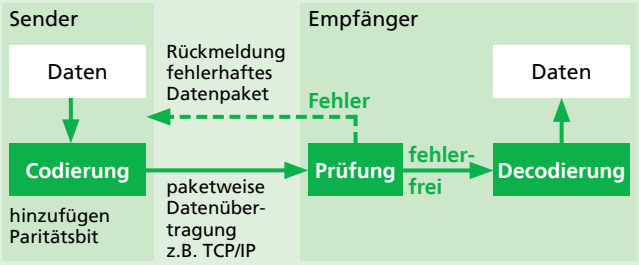
Die Anzahl möglicher Kennzeichen reicht nicht aus. Die Zulassungsstelle in Suhl muss auch Kennzeichen mit zwei Buchstaben oder vier Ziffern ausgeben.

[1)] Kraftfahrt-Bundesamt: Bestand am 1. Januar 2019 nach Zulassungsbezirken und Gemeinden
https://www.kba.de/DE/Statistik/Fahrzeuge/Bestand/ZulassungsbezirkeGemeinden/zulassungsbezirke_node.html
(Stand September 2019)

Vorwärtsfehlerkorrektur

Durch technische Probleme oder äußere Einflüsse können bei der Übertragung von Daten Fehler auftreten. Sie können zur Veränderung einzelner Bits oder ganzer Datenpakete führen. Zu einer sicheren Datenübertragung gehören daher auch Maßnahmen zur Fehlererkennung und -korrektur.

Seit den frühen 1970er Jahren beruht die Datenübertragung im Internet auf dem Protokoll TCP/IP. Sender und Empfänger stehen während der Datenübertragung über dieses Protokoll in ständigem Kontakt zueinander. Beim Empfänger werden ankommende Daten auf Fehler überprüft. Dabei werden Paritätsbits genutzt, die beim Sender im Zuge der Codierung zu den Datenpaketen hinzugefügt wurden. Wird ein Fehler festgestellt, erfolgt eine Rückmeldung an den Sender und das betreffende Datenpaket wird erneut übertragen.

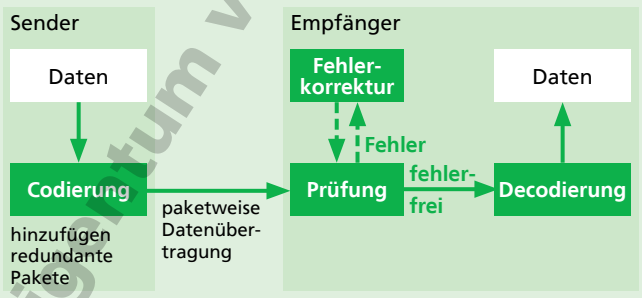


Ablaufschema Rückwärtsfehlerkorrektur

Da die Fehlerkorrektur eine Rückmeldung an den Sender erfordert, nennt man diese Art der Fehlerkorrektur auch Rückwärtsfehlerkorrektur. Sie benötigt kaum zusätzliche Übertragungskapazität, ist durch die mehrfache Übertragung fehlerhafter Pakete aber langsam.

Für Anwendungen, in denen es auf schnelle Datenübertragung ankommt, wie beim digitalen Antennenfernsehen (DVB), beim Mobilfunk oder aber auch beim Abspielen einer gewöhnlichen Audio-CD ist die Rückwärtsfehlerkorrektur daher nicht geeignet. Hier wird stattdessen die so genannte Vorwärtsfehlerkorrektur eingesetzt.

Statt eines Paritätsbits werden den Datenpaketen bei der Vorwärtsfehlerkorrektur beim Codieren zusätzliche, redundante Datenpakete hinzugefügt. Werden beim Empfänger Datenfehler festgestellt, können die fehlerhaften Datenpakete direkt beim Empfänger anhand dieser redundanten Daten wiederhergestellt werden.



Ablaufschema Vorwärtsfehlerkorrektur

Da bei der Vorwärtsfehlerkorrektur die Rückmeldungen an den Sender und die mehrmalige Übertragung einzelner Datenpakete entfallen, ist dieses Verfahren deutlich schneller. Die zusätzlich übertragenen redundanten Datenpakete benötigen jedoch zusätzliche Übertragungskapazität.

Redundanzpaket erzeugen und verlorene Pakete wiederherstellen mit dem XOR-Operator

Für das Erzeugen der Redundanzpakete wird z. B. der XOR-Operator verwendet. XOR ist die Kurzform für „eXclusive OR“ (deutsch exklusiv oder) und zählt zu den logischen Operatoren. Verknüpft man zwei Bits miteinander, ist das Ergebnis eine 1, wenn die Bits unterschiedlich sind.

0 XOR 0 = 0 1 XOR 0 = 1
0 XOR 1 = 1 1 XOR 1 = 0

Auch zwei Datenpakete lassen sich auf diese Weise Bit für Bit mit dem XOR-Operator verknüpfen:

P1	1	0	1	0	1	0	1	0
P2	0	0	1	1	0	0	1	1
P1 XOR P2	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**

Das wird für das Erzeugen von Redundanzpaketen aus mehreren verknüpften Datenpaketen genutzt.

Die drei Datenpakete P1, P2 und P3 werden beispielsweise um ein Redundanzpaket PR ergänzt, indem sie über die Formel PR = (P1 XOR P2) XOR P3 verknüpft werden.

P1	1	0	1	0	1	0	1	0
P2	0	0	1	1	0	0	1	1
P3	0	0	0	0	1	1	1	1
P1 XOR P2	1	0	0	1	1	0	0	1
PR = (P1 XOR P2) XOR P3	1	0	0	1	0	1	1	0

Kommt eines der drei Datenpakete beim Empfänger nicht an und ist bekannt, welches der drei Pakete fehlt, lässt es sich aus den übrigen drei Paketen wiederherstellen.

P1 = (PR XOR P3) XOR P2 P2 = (PR XOR P1) XOR P3
P3 = (PR XOR P2) XOR P1

Vorwärtsfehlerkorrektur

Aufgabe 1
Beschreibe den Ablauf der Vorwärtsfehlerkorrektur.

Beim Codieren werden den Datenpaketen zusätzliche, redundate Datenpakete hinzugefügt.

Beim Empfänger werden die Daten auf Fehler geprüft. Werden Datenfehler festgestellt, werden die fehlerhaften Datenpakete anhand der redundanten Daten wiederhergestellt.

Aufgabe 2
Vergleiche die Rückwärtsfehlerkorrektur und die Vorwärtsfehlerkorrektur in Bezug auf die benötigte Übertragungskapazität und die Übertragungsgeschwindigkeit.

	Rückwärtsfehlerkorrektur	Vorwärtsfehlerkorrektur
Übertragungskapazität	kaum zusätzliche Übertragungskapazität nötig	zusätzliche Kapazität für die Übertragung der Redundanzpakete nötig
Übertragungsgeschwindigkeit	gering aufgrund mehrmaliger Übertragung fehlerhafter Pakete	hoch, da alle Pakete nur einmal übertragen werden müssen

Aufgabe 3
Warum ist die Datenübertragung mittels Vorwärtsfehlerkorrektur schneller als mittels Rückwärtsfehlerkorrektur?

Rückmeldungen an den Sender und mehrmalige Übertragung fehlerhafter Datenpakete führen bei der Rückwärtsfehlerkorrektur zu einer geringen Übertragungsgeschwindigkeit.

Durch die Wiederherstellung fehlerhafter Datenpakete direkt beim Empfänger sind keine Rückmeldungen an den Sender nötig und alle Datenpakete müssen nur einmal übertragen werden. Dadurch ist die Übertragungsgeschwindigkeit höher als bei der Rückwärtsfehlerkorrektur.

Vorwärtsfehlerkorrektur

Aufgaben 4
Wie lautet das Redundanzpaket PR, das aus den folgenden Datenpaketen mit Hilfe des XOR-Operators ermittelt wird?

P1	1	0	0	1	1	0	0	1
P2	1	1	1	0	1	1	1	0
P3	0	1	0	0	1	1	0	0

P1 XOR P2	0	1	1	1	0	1	1	1
PR = (P1 XOR P2) XOR P3	0	0	1	1	1	0	1	1

Aufgabe 5
Bei der Übertragung ging das Datenpaket P3 verloren. Stelle es mit Hilfe des Redundanzpakets PR und des XOR-Operators wieder her.

P1	1	0	0	1	0	0	0	1
P2	1	1	1	0	1	0	1	1
P3								
PR	0	0	0	1	0	0	0	1

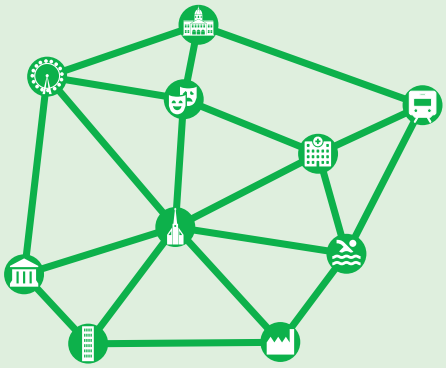
PR XOR P2	1	1	1	1	1	0	1	0
P3 = (PR XOR P2) XOR P1	0	1	1	0	1	0	1	1

Datenstruktur Graph

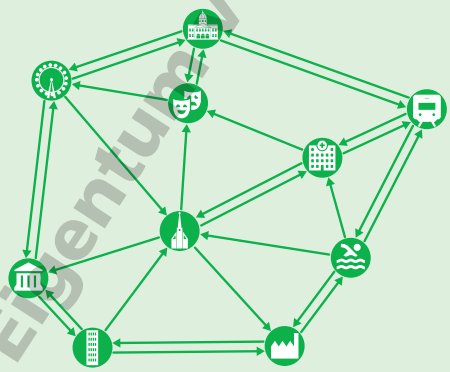
Der Graph ist eine dynamische Datenstruktur, mit der sich vernetzte Strukturen wie Straßenverbindungen, Rohrleitungs- und Telefonnetze oder auch soziale Netzwerke abbilden lassen.

Graphen bestehen aus Knoten und Kanten, die jeweils zwei Knoten miteinander verbinden. Innerhalb eines Graphen führt von jedem Knoten ein Weg zu jedem anderen Knoten.

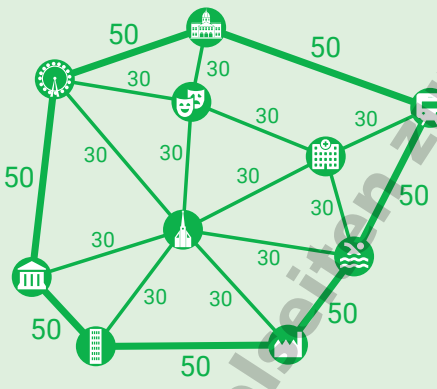
Man unterscheidet vier grundlegende Arten von Graphen:



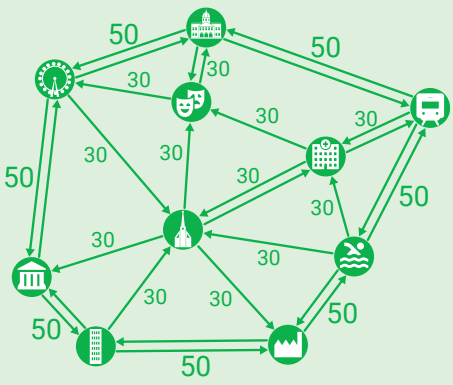
Ungerichtete Graphen zeigen nur die bestehenden Verbindungen der Knoten. In unserem Beispiel sind das die Straßen, die von einer Sehenswürdigkeit unserer kleinen Stadt zur anderen führen.



Der gerichtete Graph enthält zusätzlich Informationen über die Richtung der Verbindungen. In unserem Beispiel gibt es Einbahnstraßen und Straßen mit Gegenverkehr, die im Graph als einzelne und doppelte Pfeile dargestellt sind.



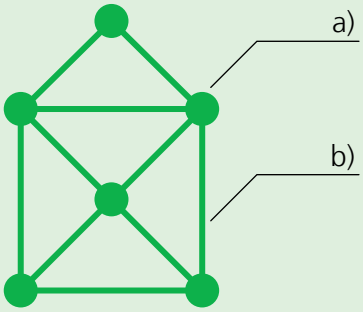
In einem ungerichteten, gewichteten Graph lassen sich Eigenschaften der Wegstrecken abbilden, die durch eine Kante repräsentiert werden. Das können beispielsweise Entfernungen in einem Straßennetz oder Durchflussmengen in einem Rohrleitungsnetz sein. In unserem Beispiel lassen sich so die unterschiedlichen zulässigen Höchstgeschwindigkeiten darstellen.



Ein gerichteter, gewichteter Graph vereint beide Möglichkeiten. In ihm lassen sich sowohl die Richtung der Verbindungen als auch Eigenschaften der Wegstrecken (Kanten) abbilden. In unserem Beispiel lassen sich auf diese Weise die Einbahnstraßen und die zulässigen Höchstgeschwindigkeiten abbilden.

Datenstruktur Graph

Aufgabe 1
Benenne die Teile des Graphen.



a) Knoten
b) Kante

Aufgabe 2
Worin besteht der Unterschied zwischen einem Baum und einem Graph?

Innerhalb eines Graphen führt von jedem Knoten ein Weg zu jedem anderen Knoten. Es gibt keine hierarchischen Beziehungen zwischen den Knoten eines Graphen. Alle Knoten sind gleichwertig.

In einem Baum besteht eine hierarchische Beziehung vom Wurzelknoten bis hinunter zu einem Blatt. Innerhalb eines Baumes gibt es von der Wurzel zu jedem Knoten einen eindeutigen Pfad.

Aufgabe 3
Nenne Beispiele aus dem Alltag, die sich mit Hilfe von Graphen darstellen lassen, und zwar als

a) ungerichteter Graph
Autobahnetz,
Stromnetz,
Soziales Netzwerk

b) gerichteter Graph
Abwassernetz mit Fließrichtung,
Straßennetz mit Einbahnstraßen
Fluchtwegplan in einem Gebäude

c) gewichteter Graph
Autobahnnetz mit Entfernungen,
Rohrleitungsnetz mit unterschiedlichen Rohrquerschnitten
Busliniennetz mit Fahrzeiten

Datenstruktur Graph

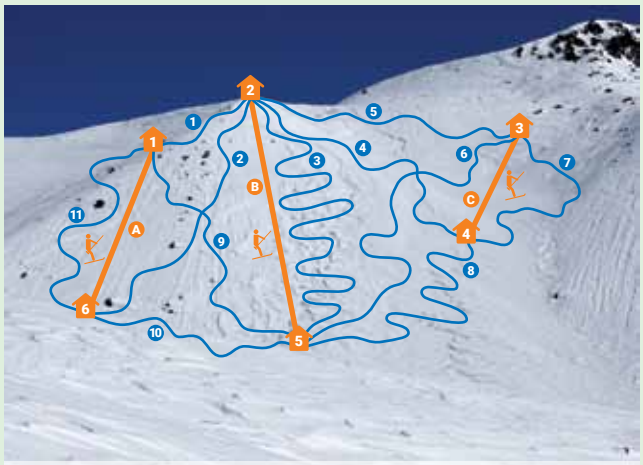
Aufgabe 4
Zeichne unser kleines Skigebiet im Bild als Graph, und zwar als

a) ungerichteter Graph

b) gerichteter Graph

c) gewichteter Graph

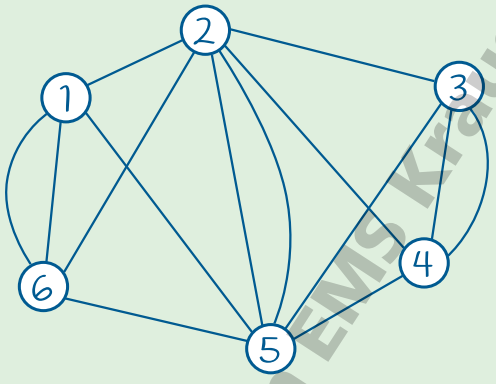
Dabei gehen wir davon aus, dass mit den Schleppliften nur bergauf und auf den Pisten nur bergab gefahren wird.



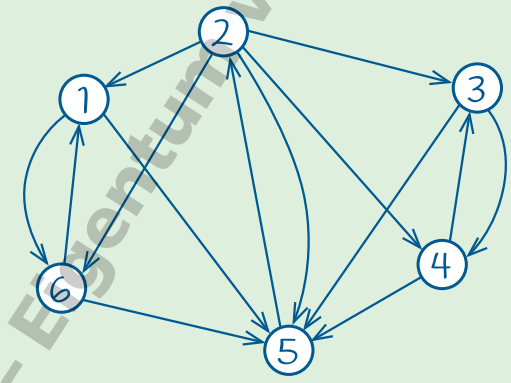
1	Lichtmoosabfahrt	800 m	8	Familienabfahrt	2500 m
2	Kitzsteinabfahrt	3300 m	9	Jägerabfahrt	2800 m
3	Sonneckabfahrt	3800 m	10	Grafenwiese	1400 m
4	Zirbentalabfahrt	3100 m	11	Schafalpeabfahrt	2700 m
5	Fuchsbergabfahrt	2600 m	A	Schafalpelift	1300 m
6	Angertalabfahrt	3500 m	B	Kitzsteinlift	2700 m
7	Breitspitzabfahrt	1500 m	C	Breitspitzlift	800 m

Foto: Natalia Kollegova (Pixabay)

a)



b)



c)