

KAPITEL 1 NACHRICHTEN



DIESES KAPITEL HANDELT VON BOB UND ALICE, VON FACKELN UND VON BUCHSTABENSALAT. Du erfährst, wie das Übermitteln von Nachrichten funktioniert und was du tun musst, damit die Nachricht geheim bleibt.

Die Geheimhaltungstricks, die wir dir zeigen, sind inzwischen ein alter Hut. Seit es Computer gibt, kann man diese Tricks schnell knacken. Aber das macht nichts, denn die alten Verfahren funktionieren nach dem gleichen Prinzip wie die neuen – und sie sind viel einfacher zu verstehen. Am allerwichtigsten: Die alten Verfahren kannst du prima selbst ausprobieren. Vielleicht kannst du damit ja für die Schule einen Spickzettel schreiben.

NACHRICHT, SENDER UND EMPFÄNGER

Stell dir vor, du möchtest jemand anderem etwas mitteilen. Steht dir dieser Jemand gleich gegenüber, dann kannst du einfach sprechen. Ist die Person weit von dir entfernt, dann benötigst du

Hilfsmittel wie Telefon oder Computer. Egal wie du etwas mitteilst, das Prinzip ist immer dasselbe.



Die Information, die du austauschst, wird Nachricht genannt. Die Person, die die Nachricht übermittelt, ist der Sender. Die Person, für die die Nachricht bestimmt ist, ist der Empfänger. Der Sender spricht. Der Empfänger hört zu. Das Ganze nennt man Kommunikation.



In Informatik-Fachbüchern werden Sender und Empfänger meist Alice und Bob genannt. Alice will eine Nachricht an Bob senden. Das ist schöner, als die Beteiligten einfach Person A und Person B zu nennen.

Immer, wenn du eine Nachricht sendest, musst du für zwei Dinge sorgen:

- » Sie muss beim Empfänger ankommen.
- » Der Empfänger muss sie verstehen.

Bei einem normalen Gespräch überträgt der Schall in der Luft deine Nachricht. Würdest du das auf dem Mond versuchen, dann hättest du ein Problem mit der Übertragung – es gibt keine Luft.

Ein Tourist spricht dich in seiner Sprache an. Du verstehst ihn nicht. Vielleicht könnt ihr euch zur Übertragung der Nachricht auf Englisch einigen – wenn ihr das beide versteht.



Nachrichten müssen immer in eine übertragbare Form gebracht werden. Sie werden codiert. Ein Code ist die Übertragungsform einer Nachricht.

Beim Empfänger werden Nachrichten wieder decodiert.

Neben unserer Sprache und anderen Sprachen gibt es noch viele andere Codes:

- » Ein tauber Mensch kann keinen Schall hören, er verwendet eine besondere Sprache – die Gebärdensprache. Gebärdensprache ist ziemlich kompliziert, das **Fingeralphabet** kannst du schneller erlernen.

H – A – L – L – O



Aufgabe 1 Hinten im Buch findest du alle Zeichen des Fingeralphabets. Schreibe auf, welche Nachricht hier übermittelt wird.



Aufgabe 2 Zeige Alex das Wort CODE im Fingeralphabet.

- » Im Morsealphabet werden alle Buchstaben des Alphabets mit Punkten und Strichen dargestellt. Für die Punkte und Striche kannst du auch kurze und lange Lichtsignale senden. Das geht besonders gut nachts mit einer Taschenlampe.

HALLO

.... - - - - - - -



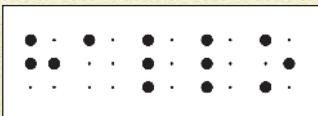
Aufgabe 3 Hinten im Buch findest du alle Zeichen des Morsealphabets. Schreibe auf, welche Nachricht hier übermittelt wird.

... --- ...

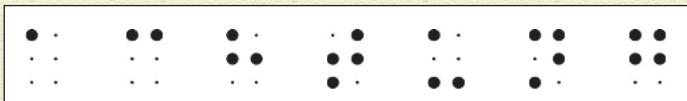


Aufgabe 4 Schreibe für Alex das Wort MORSE im Morsealphabet auf. Das geht übrigens auch mit Klopfen – mit langen und kurzen Abständen.

- » Auf Schildern im Museum siehst du außer der Schrift oft noch Punkte. In neuen Fahrstühlen stehen neben den Tasten Punkte. Auch auf Medikamentenpackungen sind diese Punkte fühlbar. Das ist die Blindenschrift (auch: Braille-Schrift).



Aufgabe 5 Hinten im Buch findest du alle Zeichen der Braille-Schrift. Schreibe auf, welche Nachricht hier übermittelt wird.



Für Profis: Schreibe für Alex das Wort BRAILLE in Braille-Schrift auf.

» Ihr landet mit einem Flugzeug im Urlaubsort. **Symbole und Schilder** weisen euch den Weg, zum Beispiel zum Schließfach.



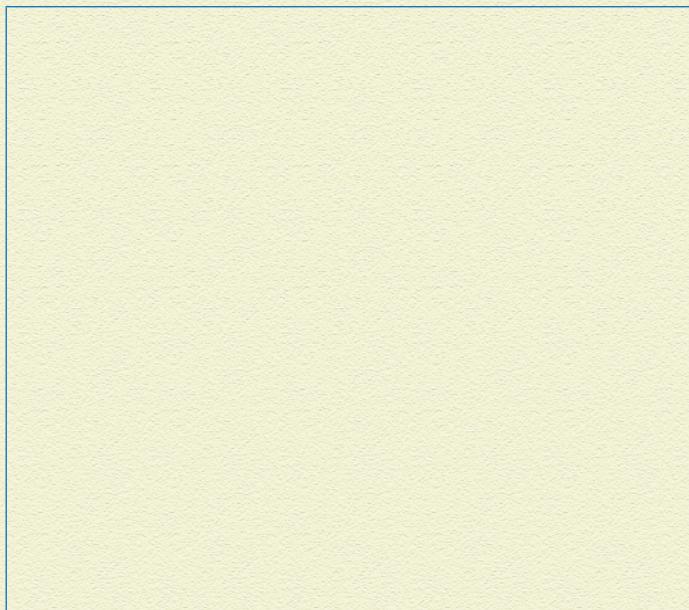
Aufgabe 6 Wo führen euch diese Schilder hin?







Aufgabe 7 Entwirf ein Schild für dein Kinderzimmer.



»



Der Kassierer im Supermarkt scannt den Einkauf. Die Nachricht, nämlich um welches Produkt es sich handelt, ist im **Strichcode** versteckt.



EAN UND ISBN

Hinter dem Strichcode verbirgt sich ein zweiter Code, die EAN (Europäische Artikel-Nummer) oder bei Büchern die ISBN (Internationale Standard-Buch-Nummer). Damit werden Artikel und Bücher eindeutig gekennzeichnet. Die aktuellen Nummern sind immer 13-stellig. Du kannst im Internet zu jeder Nummer den Artikel oder das Buch finden.



Aufgabe 8 *Hol dir aus dem Bad die Zahnpastatube. Gib in eine Suchmaschine im Internet die EAN der Tube ein. Stimmt's?*



Aufgabe 9 *Suche im Internet nach der ISBN des Buches »Kryptografie für Dummies«. In dem Buch geht es übrigens auch um den Austausch von geheimen Nachrichten. Allerdings ist das Buch für Studierende geschrieben.*

NACHRICHTEN AUSTAUSCHEN – FACKELTELEGRAF

Schon in der Antike haben Boten – meist Reiter – Nachrichten über große Entfernungen übermittelt. Noch schneller ging es mit Licht.

Licht ist über große Entfernungen gut sichtbar. Hatte ein Heer eine Schlacht gewonnen, so wurde ein Feuer auf einem hohen Berg angezündet. Auf dem nächsten Berg konnte man das sehen. Natürlich musste vorher verabredet werden, welche Bedeutung das brennende Feuer hat.



AUCH HEUTE NOCH WICHTIG: LEUCHTSIGNALE

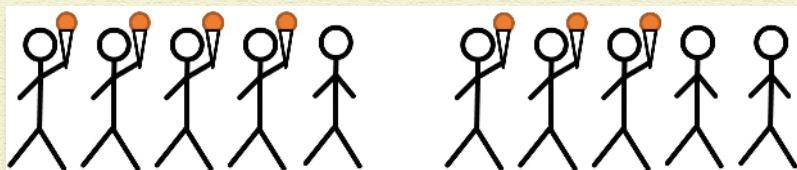
Noch heute senden
Leuchttürme Lichtsignale
weit auf das Meer hinaus.
Sie zeigen dem Seefahrer
an, wo sich das Schiff
befindet, oder welcher
Bereich für das Schiff
befahrbar ist.



Will man eine Nachricht aus Buchstaben mit Licht übertragen, muss man sich überlegen, wie das gehen soll. Ein Beispiel dafür ist der Fackeltelegraf. Die Zahl der Fackeln gibt an, welcher Buchstabe des Alphabets gemeint ist. Dabei hat der Sender zwei Gruppen von Fackeln zur Verfügung.

Man benötigt 10 Fackeln – 5 auf der linken Seite des Senders und 5 auf der rechten Seite.

Wenn du 4 Fackeln auf der linken Seite und 3 Fackeln auf der rechten Seite (kurz: 4-3) siehst, dann ist der **Buchstaben »S«** gemeint.



Wie die Kombinationen von Fackeln den Buchstaben des Alphabets zugeordnet sind, kannst du in dieser Tabelle ablesen:

		rechte Seite				
		1	2	3	4	5
linke Seite	1	A	B	C	D	E
	2	F	G	H	I/J	K
	3	L	M	N	O	P
	4	Q	R	S	T	U
	5	V	W	X	Y	Z



In der Tabelle siehst du die Fackeln vom Empfänger aus. Der Sender steht hinter den Fackeln. Er muss die Buchstaben genau seitenverkehrt übermitteln.

Solch einen Fackeltelegrafen kannst du ganz einfach **selbst bauen**.
Du brauchst dafür:

- » 10 Teelichte
- » für jedes Teelicht einen Sichtschutz



Der Sichtschutz macht dir die Sache leichter. Dann musst du die Kerzen für den nächsten Buchstaben nicht immer auspusten und wieder anzünden.



Nimm ein Abflussrohr aus dem Baumarkt und zersäge es in 10 Teile. In diesen Teilen kannst du das Teelicht verstecken, wenn du es gerade nicht brauchst. Du kannst die Teelichte aber auch hinter Bauklötzen verstecken.

Das **Lichtsignal 2-3** bedeutet, dass du in der zweiten Zeile der Tabelle den dritten Buchstaben suchen musst. Hier wird also der Buchstabe »H« (links: 2, rechts: 3) übertragen.



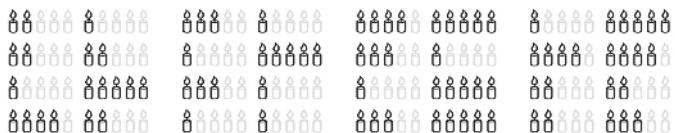


Aufgabe 10 Welches Wort wird hier übertragen?





Aufgabe 11 Welche Nachricht übermitteln wir dir hier?
Lies die Zeichen zeilenweise und schreibe sie unten auf.



Jetzt kannst du selbst loslegen. Probiere deinen Fackeltelegrafen mit Alex aus. Du bist der Sender, Alex der Empfänger.



Ihr braucht jetzt Schreibzeug.

Für dich als Sender gilt:

- 1 Schreibe zuerst deinen Text auf.**
- 2 Wandle jeden Buchstaben in ein Zeichen des Fackelalphabets um.**
- 3 Übertrage alle Fackelzeichen an Alex.**



Seitenverkehrt, du bist der Sender!



Am besten machst du nach jedem übertragenen Zeichen eine kleine Pause. Decke dazu einfach alle Teelichte ab und natürlich sendest du am besten, wenn es dunkel ist.

Für Alex als Empfänger gilt:

- 1 Schreibe die empfangenen Zeichen auf.**
- 2 Wandle die Zeichen wieder in Buchstaben um.**
- 3 Setze die Buchstaben zu der Nachricht zusammen.**



Aufgabe 12 Übermittel das Wort LICHT.

Welche Entfernung könnt ihr mit dem Fackeltelegrafen überbrücken? 25 Meter sollten möglich sein. Viel Spaß beim Fackeln! . . . und vergiss nicht, dass du auch mal schlafen musst.

GEHEIMNISSE AUSTAUSCHEN – SKYTALE

Nun, wie war das Ausprobieren des Fackeltelegrafen? Hat der Nachbar neugierig über den Gartenzaun geschaut und alles »mitgelesen«?

Manchmal möchtest du nicht, dass ein anderer mitkriegt, wovon du sprichst – du möchtest das Gespräch geheim halten. Aber: Schall kann jeder hören, Funk kann jeder empfangen und auch das Licht des Fackeltelegrafen können alle sehen.



In Fachbüchern wird die mithörende Person – neben Alice und Bob – ganz verschieden genannt: Carol, Dave, Marvin, Oscar oder Trudy. Jeder Name steht für eine andere Form der Spionage.

Du musst zusätzlichen Aufwand treiben, damit du deine Nachricht geheim halten kannst.

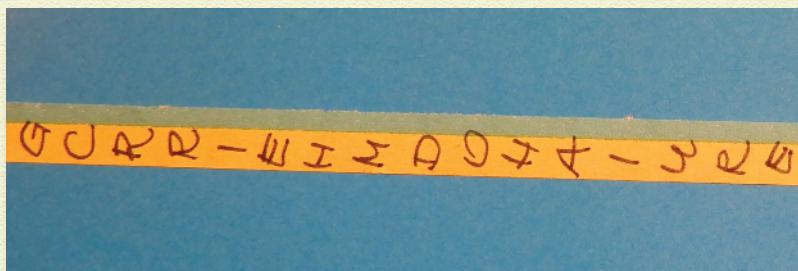


Eine Nachricht in eine geheime Form zu bringen heißt, sie zu verschlüsseln oder zu chiffrieren. Dazu brauchst du einen Schlüssel und ein Verschlüsselungsverfahren.

Die »alten Griechen« benutzten die **Skytale** zum Geheimhalten von Nachrichten. Sie nahmen einen Stab und wickelten ein Band aus Leder oder Stoff darum. Jetzt lagen mehrere Streifen Band nebeneinander. Dann schrieben sie die Nachricht zeilenweise auf das Band – auf jeden Streifen einen Buchstaben. Waren die Zeilen zu Ende, dann ging es darunter weiter.



Nach dem Beschriften der Skytale wurde das Band wieder abgewickelt und irgendwie (als Schnürsenkel, als Stirnband, als Gürtel ...) zum Empfänger gebracht. Die Buchstaben standen »wild« **durcheinander** – keiner konnte darin die Nachricht erkennen. Jedenfalls nicht so schnell.



Der Empfänger wickelte das Schriftband wieder um einen Stab und konnte die Nachricht wieder lesen. Wichtig: Der Stab musste genauso dick sein wie der Stab beim Beschriften. Hatte der Empfänger **nicht den richtigen Stab**, so hatte er nach dem Aufwickeln immer noch Buchstabensalat.



Für deine Skytale brauchst du folgendes Material:

- » einen möglichst dicken Stift als Stab
- » eine Luftschlange
- » einen Stift zum Beschriften



Nimm einen Stift mit Kappe. Die Luftschlange kannst du dann mit der Stiftkappe befestigen, dann rutscht sie nicht immer weg.

Für dich als Sender gilt:

- 1 Wickle die Luftschlange um den Stift.**
Schreibe auf jeden Streifen einen Buchstaben.
- 2 Beschriffe die Skytale von links nach rechts (zeilenweise).**
- 3 Wickle die Luftschlange wieder ab.**
- 4 Schicke das Band an Alex.**

Für Alex als Empfänger gilt:

1 Wickle die Luftschlange um einen Stift, der genauso dick ist wie der erste.

Wenn du den Text lesen kannst, hast du alles richtig gemacht.



VERSCHLÜSSELN MIT DER SKYTALE

- » Verschlüsselungsverfahren: Band um einen Stab wickeln und draufschreiben.
- » Schlüssel: Durchmesser des Stabs. Falscher Durchmesser – keine Entschlüsselung.

Jetzt kannst du geheime Botschaften sogar sicher über große Entfernungen übermitteln. Dazu musst du erst deine Nachricht mit der Skytale verschlüsseln und dann die Buchstaben in der Reihenfolge auf dem Band mit dem Fackeltelegrafen übertragen.

Du hast deine Nachricht übertragen, ein Fremder konnte sie zwar »mitlesen« – er konnte aber damit nichts anfangen. Deine Nachricht ist sicher.

- » Das Codieren (mit dem Fackeltelegrafen) sorgt dafür, dass die Nachricht übermittelt werden kann.
- » Das Chiffrieren (mit der Skytale) sorgt zusätzlich dafür, dass die Nachricht auch geheim bleibt und niemand Unbefugtes die Nachrichten verstehen kann.

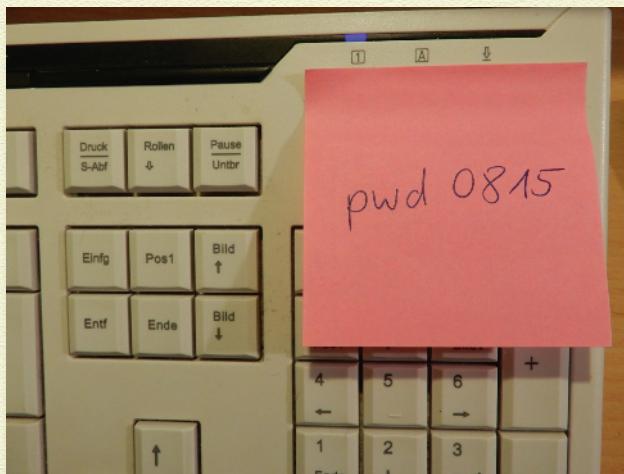
GEHEIMNISSE BEWAHREN – PASSWORTE

Damit deine chiffrierte Nachricht nicht geknackt werden kann, musst du den Schlüssel gut aufbewahren. Genauso wie du dein Smartphone und den Computer vor unberechtigtem Zugriff schützen musst, damit niemand an deine Informationen, die dort gespeichert sind, gelangen kann.

Es gibt mehrere Möglichkeiten, wie du dafür sorgen kannst, dass kein Fremder Zugang zu deinem Gerät bekommt:

- » Fingerabdruckscanner
- » Mustererkennung
- » Gesichtserkennung
- » Passwort

Am einfachsten ist es dabei für einen Fremden sicherlich, das Passwort herauszubekommen. Manchmal genügt es schon, den Sender einer Nachricht genau zu kennen oder ihn nur zu beobachten. Oft macht dieser einen Fehler, ohne ihn selbst zu merken. **Solche Fehler** können ganz schnell geschehen.





SCHNELL PASSIERT!

Deine Schwester möchte Videos mit Freundinnen austauschen und hat sich bei einem Videokanal anmeldet. Beim Anmelden hat sie selbst ein Passwort festgelegt. Damit sie es nicht vergisst, hat sie es aufgeschrieben – der Zettel liegt noch auf dem Schreibtisch.

Du chattest gerade mit deinen Großeltern und fotografierst deine Schwester vor dem PC. Dann sendest du das Bild. Was du gar nicht bemerkt hast – auf dem Foto ist das Passwort deutlich zu lesen.

Wer hat hier eigentlich einen Fehler gemacht? Stell dir vor, was geschieht, wenn dieses Passwort in die falschen Hände gerät.



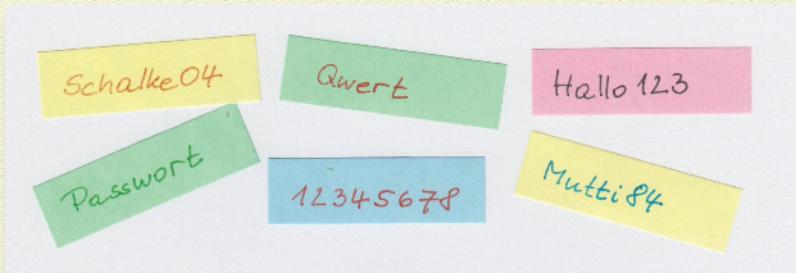
Passwörte sind Schlüssel für den Zugang zu Computersystemen. Mit ihnen erhältst du die Erlaubnis, auf dem System zu arbeiten.

Leider werden Passwörte sehr oft aufgeschrieben und dann bleibt der Zettel auch noch in der Nähe des Computers liegen. Manchmal klebt der Zettel sogar am Bildschirm des Computers.



Lass ein Passwort niemals offen liegen.

Oft machen sich Nutzer aber auch zu wenig Gedanken bei der Vergabe eines Passworts. Sie sind zu bequem, sich ein sicheres Passwort auszudenken und zu merken. Dann tippen sie auf Tasten, die auf der Tastatur nebeneinanderliegen, oder wählen Begriffe, die sie sich leicht merken können – zum Beispiel weil sie Fußballfan sind. Wenn man den Nutzer kennt, kann man das Passwort leicht erraten. **Manche Passworte werden besonders häufig verwendet.**



Verwende sichere Passworte.

Das Bundesamt für Sicherheit in der Informationstechnik hat Richtlinien für gute Passworte veröffentlicht:

- » Je länger, desto besser (aber mindestens 8 Zeichen lang) – das vergrößert den Aufwand für den Angreifer.
- » Verwende alle Zeichen, also: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen – das macht es für den Angreifer komplizierter.
- » Benutze keine Namen und Worte – diese Worte können erraten werden, wenn man den Nutzer kennt.
- » Hänge Ziffern und Sonderzeichen nicht einfach an ein Wort an – das Wort macht das Passwort unsicher.
- » Benutze keine nebeneinanderliegenden Tasten.



Aufgabe 13 Kreuze an, welches Passwort sicher ist und welches unsicher. Begründe, wenn ein Passwort nicht sicher ist.

Mama4711

Sicher.

Unsicher, weil _____

MIMha#2412Gt

Sicher.

Unsicher, weil _____

(Lisa)0815

Sicher.

Unsicher, weil _____

qayxsw9876

Sicher.

Unsicher, weil _____

mein+langes*Geheimes#Passwort

Sicher.

Unsicher, weil _____

ek84RT02#"

Sicher.

Unsicher, weil _____

lwidBs\$15

Sicher.

Unsicher, weil _____

o3A;w

Sicher.

Unsicher, weil _____

Wie kannst du dir aber ein so langes Passwort merken, das noch dazu Ziffern und Sonderzeichen enthält? Da gibt es einen einfachen Trick.



Wenn du ein Passwort festlegst, dann denke dir eine Geschichte oder einen Satz dazu aus.

Mit einem passenden Satz fällt es dir leicht, dir auch scheinbar schwierige Passworte zu merken.

MIMha#2412Gt Hier versteckt sich der Satz »Meine liebe Mama hat am 24.12. Geburtstag«.

IwidBs\$15 »Ich wohne in der Burgstraße Nummer 15.«

ek84RT02#“ OK, hier fällt uns kein sinnvoller Satz ein. Solche sicheren Passworte werden meist von Computern erzeugt. Oft kannst du das Passwort dann ändern. Vergiss aber die Richtlinien nicht.