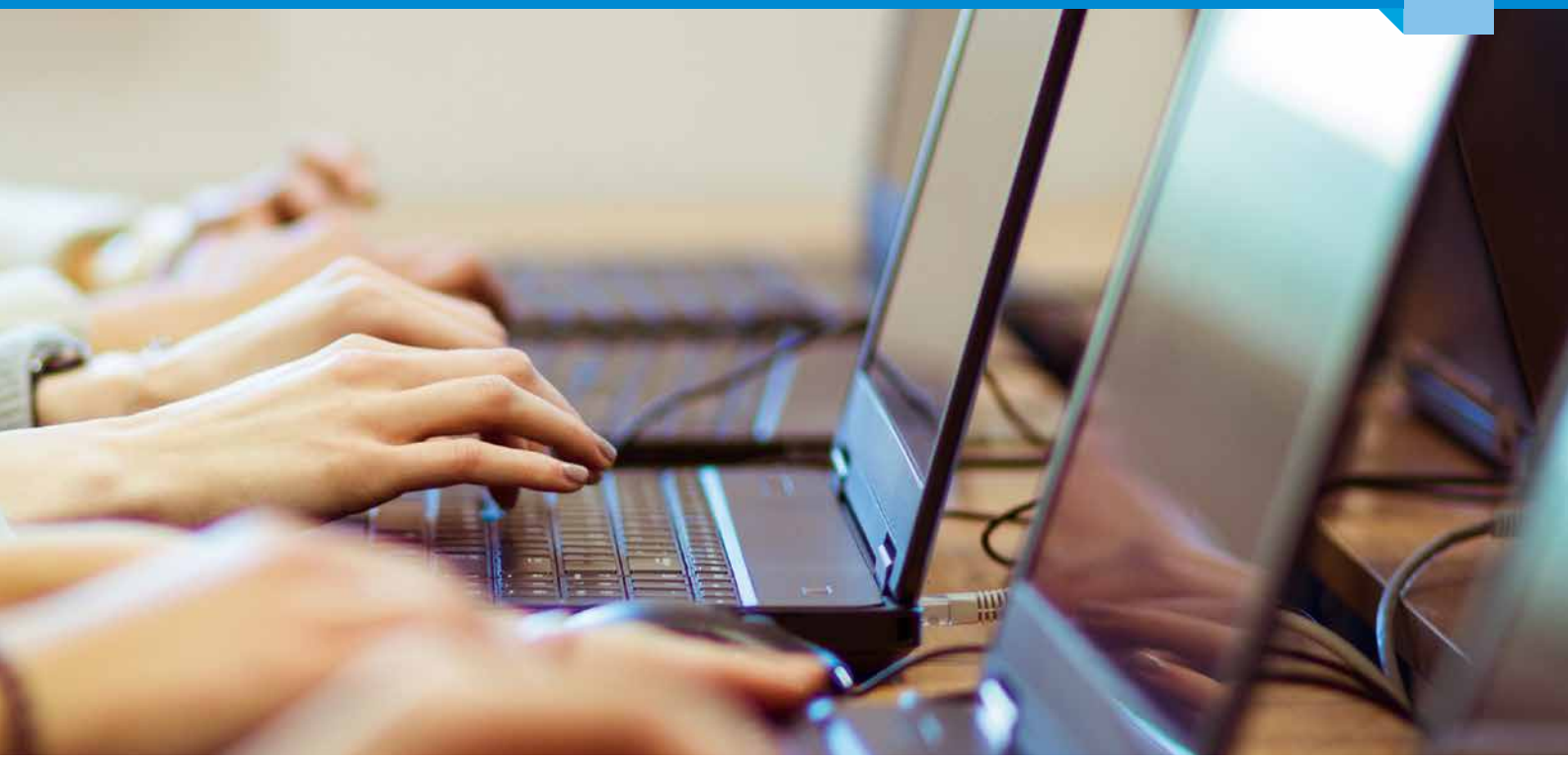
Informatik 9/10

kostenfreie **LESEPROBE**

C.C.BUCHNER

Gymnasium
Nordrhein-Westfalen

Inhalt



Liebe Lehrerinnen und Lehrer,

in diesem Jahr setzen wir unsere Reihe **Informatik – Nordrhein-Westfalen** mit **Informatik 9/10** fort und bieten Lehrkräften an nordrhein-westfälischen Gymnasien ein Lehrwerk, das die Anforderungen des aktuellen Kernlehrplans passgenau umsetzt.

Unser **digitales Lehrermaterial click & teach** unterstützt Sie optimal bei der Gestaltung Ihres Unterrichts und bietet zahlreiche Zusatzmaterialien wie Lösungen, Arbeitsblätter, Erklärfilme und vieles mehr. Selbstverständlich erscheint **Informatik 9/10** auch als **digitale Ausgabe click & study** für Ihre Schülerinnen und Schüler.

Wenn Sie mehr über **Informatik – Nordrhein-Westfalen** erfahren möchten, kontaktieren Sie uns! Wir beraten Sie gern!

Herzlichst
Ihr Schulberatungsteam für Nordrhein-Westfalen

Monika Labmeier
Mobil: 0171 6357092
E-Mail: labmeier@ccbuchner.de

Jutta Schneider
Mobil: 0175 3248279
E-Mail: schneider@ccbuchner.de

Jörn Thielke
Mobil: 0160 1728354
E-Mail: thielke@ccbuchner.de

Entdecken Sie die Lehr- und Lernwelt von …

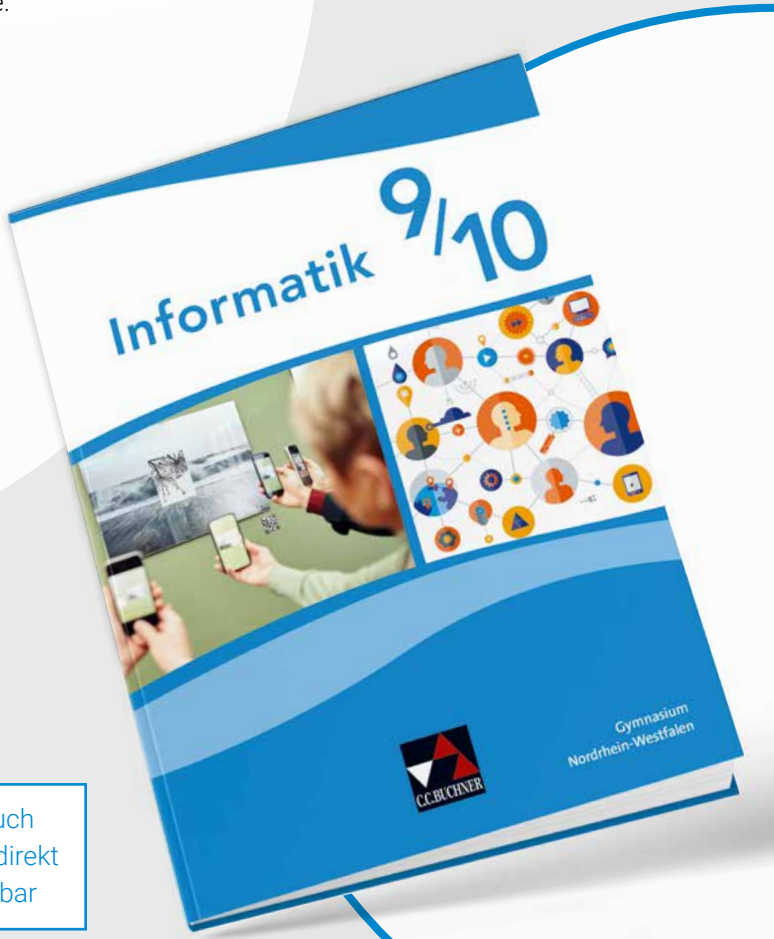
Informatik – Nordrhein-Westfalen

Informatik 9/10
Gymnasium

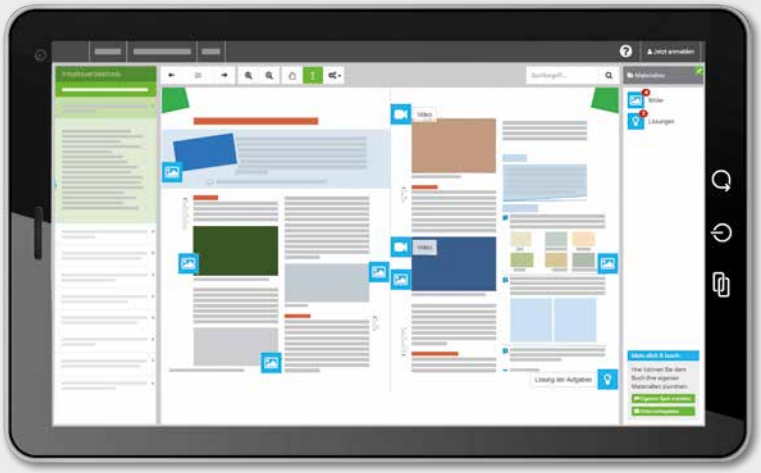
Das Lehrwerk setzt auf eine praxisnahe und anwendungsbezogene Umsetzung der im Kernlehrplan vorgesehenen Inhalte. Auf Lehrkräfte sowie Schülerinnen und Schüler warten spannende Themen wie:

- Codierung und Decodierung verschiedener Verschlüsselungen von der Antike bis zur Neuzeit
- projektorientiertes Arbeiten mit Python und dem Calliope
- Einblicke in die Welt der Künstlichen Intelligenz
- Entwicklung einer eigenen Website vom Konzept bis zur Umsetzung

Mehr Infos
www.ccbuchner.de/bn/38043



digitales Zusatzmaterial auch via QR- oder Mediencodes direkt in der Print-Ausgabe verfügbar



click & teach click & study

Ideal für den digitalen Materialaustausch

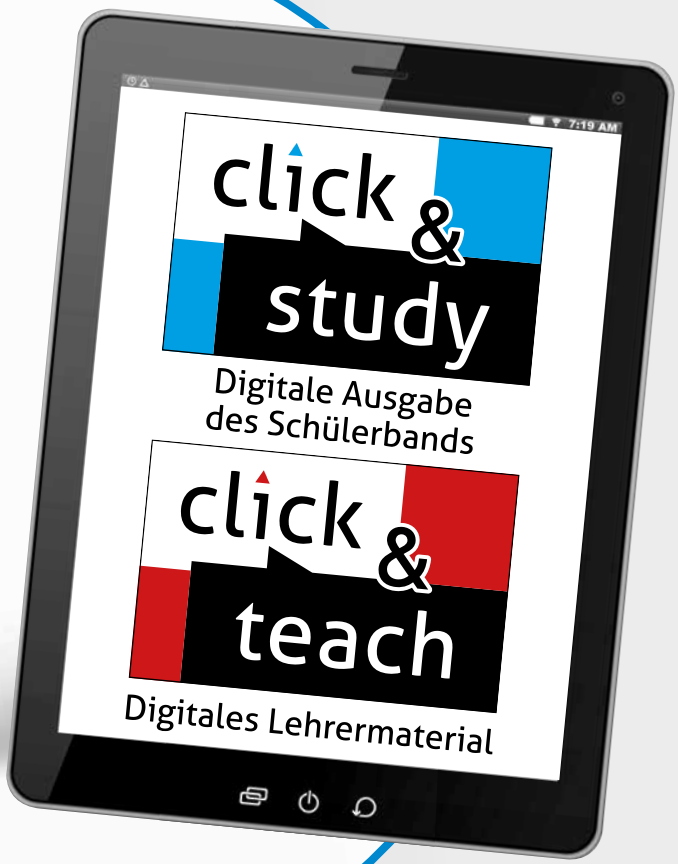
Die **digitale Ausgabe des Schülerbands click & study** und das **digitales Lehrermaterial click & teach** bilden zusammen die ideale digitale Lernumgebung: vielfältig im Angebot und einfach in der Bedienung!

Mehr Infos finden Sie auf den Seiten 38 bis 41 und auf www.click-and-teach.de und www.click-and-study.de.

Demoversion
click & teach 5/6

Informatik – Nordrhein-Westfalen punktet durch:

- informative Erarbeitungstexte
- Unterstützung der Darstellung durch visuelle Elemente
- weiterführende Materialien zur Vertiefung und Erweiterung der behandelten Inhalte
- umfangreiches Aufgabenangebot zur Auswahl
- vielseitige Einführung in Programme zur Anwendung des Unterrichtsinhaltes



Praxisorientierte Kapitel für einen realitätsnahen Informatikunterricht!

Jedes Kapitel zeichnet sich durch einen hohen Praxisbezug sowie integrierte Projekte und Anwendungen aus. So setzen sich die Schülerinnen und Schüler im Kapitel „Webdesign" beispielsweise mit dem Thema HTML auseinander und können am Kapitelende ihre eigene Website erstellen.

Jetzt testen!

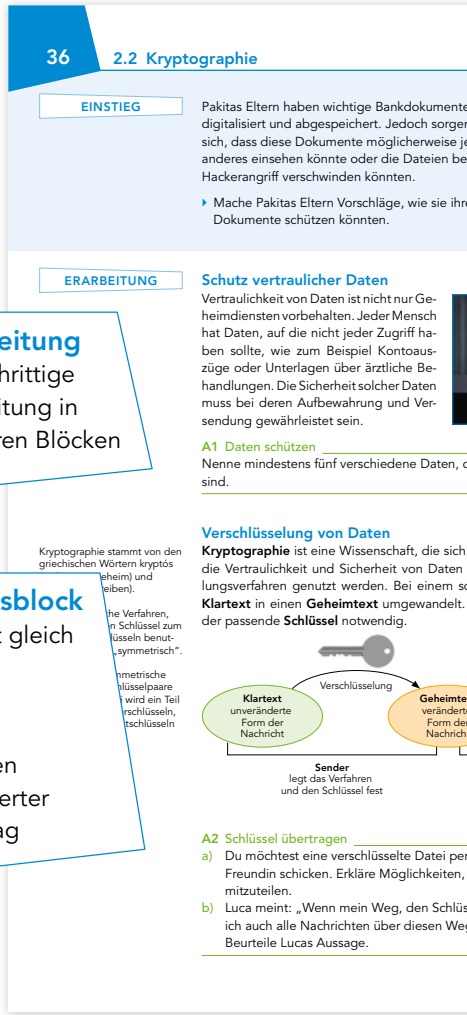
click & study als Print-Plus-Lizenz
ab 2,20 € pro Titel und Jahr
bei Einführung der Print-Ausgabe

Informatik – Nordrhein-Westfalen	ISBN 978-3-661- / Bestellnr.	Ladenpreis	Lieferbarkeit
Informatik 9/10	38043-8	ca. 28,– €	4. Quartal 2024
click & study 9/10 Digitale Ausgabe Informatik 9/10	WEB 380431 Bestellbar auf www.ccbuchner.de	ca. 8,50 €	4. Quartal 2024
click & teach 9/10 Einzellizenz Digitales Lehrermaterial	WEB 380531 Diese und weitere Lizenzarten finden Sie auf www.ccbuchner.de		in Vorbereitung

Aufbau der Kapitel

Auftaktseite
Abholen im Alltag und Ausblick auf die neuen Kompetenzen

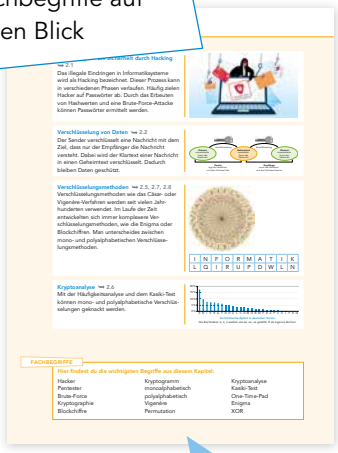
Einstieg
motivierende Fragen zum neuen Thema



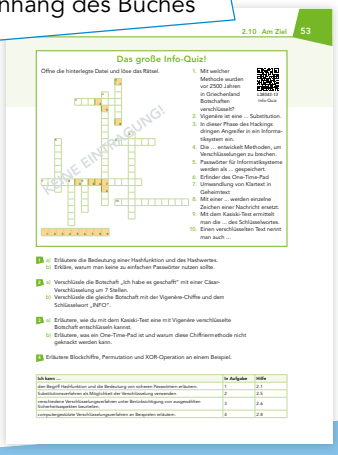
Erarbeitung
kleinschrittige Erarbeitung in mehreren Blöcken

Erarbeitungsblock
Jeder Block ist gleich aufgebaut:
- Überschrift
- kompakte Informationen
- praxisorientierter Arbeitsauftrag

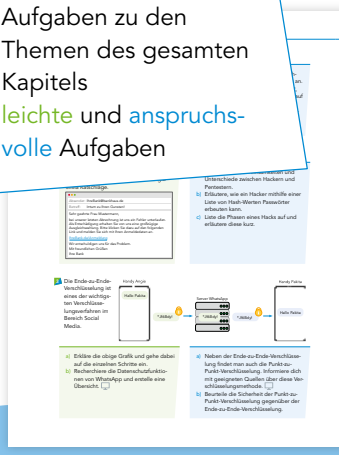
Alles im Blick
die wichtigsten Inhalte und Fachbegriffe auf einen Blick



Am Ziel
- Sitzen alle neuen Basiskompetenzen?
- Lösungen im Anhang des Buches



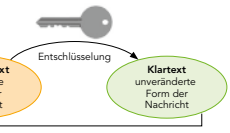
Üben und Vertiefen
- paralleldifferenzierte und vernetzende Aufgaben zu den Themen des gesamten Kapitels
- leichte und anspruchsvolle Aufgaben



Alle Doppelseiten zum Erwerben neuer Kompetenzen haben diesen Aufbau.

die deiner Meinung nach schützenswert

mit Verschlüsselungen beschäftigt. Um
zu gewährleisten, können Verschlüsse-
olchen Verfahren wird ein sogenannter
Für die Ver- und Entschlüsselungen ist



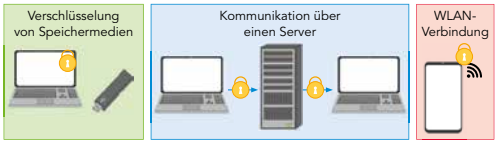
Empfänger
muss das Verfahren
und den Schlüssel kennen

E-Mail an einen Freund oder eine
dieser Person den Schlüssel gefahrlos

sel zu übertragen, sicher ist, dann kann
g übertragen."

Anwendungen von Verschlüsselungstechnologie

Verschlüsselungen werden in vielen Situationen eingesetzt, in denen Daten digital gespeichert und übertragen werden:



Die Art der Verschlüsselung hängt dabei vom Anwendungsfall ab. Die Sicherheit einer Verschlüsselung hängt jedoch immer von der Anzahl der möglichen Schlüsselkombinationen ab. Die Nutzung des Internets würde ohne Verschlüsselung nicht funktionieren.

A3 Verschlüsselungstechnologien zuordnen

Datenträger	WLAN	Browser	E-Mail	Messenger
BitLocker (Microsoft) FileVault (Apple) VeraCrypt (Open Source)	WPA2 WPA3	SSL TLS	PGP X.509	Signal Protocol Whatsapp Protocol Skype Protocol

MERKE

Kryptographie beschäftigt sich mit Methoden, Daten zu **verschlüsseln**, um deren Vertraulichkeit zu schützen. Eine Verschlüsselung wandelt **Klartext** mithilfe eines **Schlüssels** in einen **Geheimtext** um. Die Originaldaten können nur mithilfe des passenden **Schlüssels** wiederhergestellt werden können.

AUFGABEN

1 a) Wähle dich mit einem Endgerät, z. B. deinem Handy, in ein WLAN ein. Prüfe und nenne die verwendete Verschlüsselungsmethode.
b) Recherchiere die Verbesserungen der Sicherheit bei der WPA3-Methode gegenüber der WPA2-Methode.
c) Recherchiere und erkläre die Rolle eines Radius-Servers im Zusammenhang mit der Verschlüsselung eines WLANs.

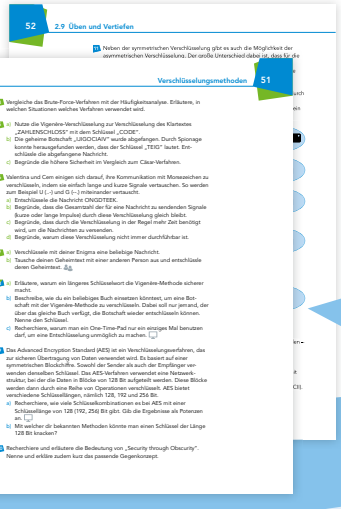
2 a) Viele Messenger-Dienste verwenden eine „Ende-zu-Ende-Verschlüsselung". Recherchiere und erkläre diese Verschlüsselungsmethode.
b) Erläutere auf Grundlage deiner Recherche, wie sich Ende-zu-Ende von der Verschlüsselung zwischen Browser und Webserver unterscheidet.

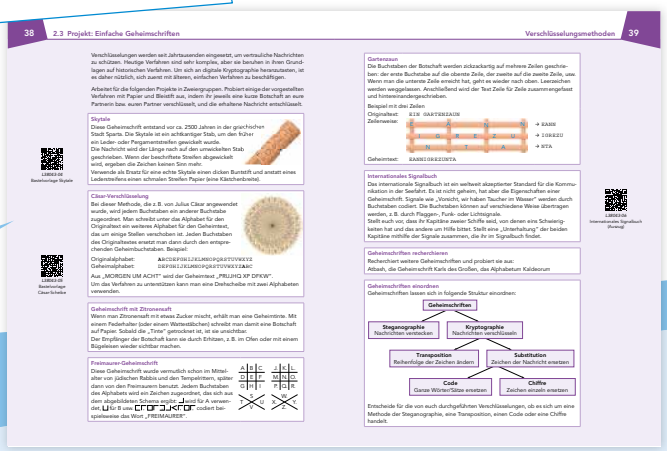
3 Bei modernen Verschlüsselungsverfahren ist das automatisierte Durchprobieren aller Schlüssel die einzig mögliche Angriffsmethode. Gehe von einem modernen PC aus, der rund 2 Milliarden Schlüssel pro Sekunde testen kann. Berechne die Zeit, die zum Testen aller Schlüssel benötigt wird:
a) Der Schlüssel besteht aus sieben Kleinbuchstaben.
b) Der Schlüssel besteht aus acht Großbuchstaben.
c) Der Schlüssel besteht aus acht Zeichen (Klein- und Großbuchstaben und die Ziffern von 0 bis 9).

Merke
das Wichtigste in Kürze

Übungsaufgaben
- leichte und anspruchsvolle Aufgaben zu den Inhalten dieser Doppelseite
- Symbole kennzeichnen Arbeit mit einem Endgerät, Partner- und Gruppenarbeiten.
- QR-Codes liefern zusätzliche Materialien für Aufgaben, H5P-Varianten oder Links zu externen Inhalten

Projekt
spannende Projekte zum Vertiefen und Anwenden





9/10 Informatik

Bearbeitet von
Andre Asschoff
Christian Bader
Carsten Dittich
Christian Pothmann

C.C.Buchner

4 Inhaltsverzeichnis

6 Inhaltsverzeichnis

2 Verschlüsselungs-methoden

Einstieg

Wie kann man geheime Informationen geheim halten? Im modernen Informationszeitalter wird es immer schwieriger, bestimmte Informationen zu verschlüsseln und vor unbefugtem Zugriff zu schützen.

- Finde Situationen, in denen es wichtig ist, Informationen zu schützen.
- Nenne mögliche Verschlüsselungen, die du aus den Jahrgangsstufen 5/6 bereits kennst.

Am Ende dieses Kapitels hast du gelernt, …

- was man unter dem Begriff „hacken" versteht.
- welche unterschiedlichen Verschlüsselungsmethoden es gibt.
- worauf es bei modernen Verschlüsselungsmethoden ankommt.

34 2.1 Bedrohung für die Sicherheit durch Hacking

EINSTIEG

L38043-01
Grafik zum Lagebericht des BSI

Das Bundesamt für Sicherheit in der Informationstechnik erstellt jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland. In der hinterlegten Grafik wird dieser Bericht in einer Grafik zusammengefasst.

- Verschaffe dir damit einen Überblick über Bedrohungen, die gerade aktuell sind.

Bundesamt für Sicherheit in der Informationstechnik

ERARBEITUNG

Hacker und Pentester

Während **Hacking** ursprünglich dafür steht, Lösungen für knifflige Probleme (durch Programmierung von Computern) zu finden, wird der Begriff heute meist für das illegale Eindringen in Informatiksysteme verwendet. Dabei können z. B. Daten gestohlen oder die Verfügbarkeit eines Systems außer Kraft gesetzt werden. Hinter Hacking-Angriffen stehen unterschiedliche Absichten, u. a. Bereicherung durch Diebstahl oder Erpressung, Manipulation der öffentlichen Meinung, Behinderung eines Gegners in Konflikten oder Kriegen, Spionage und manchmal auch einfach Abenteuerlust.

Auch sogenannte Whistle-Blower verschaffen sich (zum Teil illegal) Zugriff auf Daten, wobei ihre Absicht aber das Bloßstellen unlauterer bzw. krimineller Machenschaften ist.

Hacker müssen nicht kriminell sein: **Pentester** werden von Unternehmen engagiert, um gezielt nach Schwachstellen in der Sicherheit ihrer Informatiksysteme zu suchen, damit Sicherheitslücken geschlossen werden können.

pen: Abk. für penetration (engl. für Eindringen in Informatiksysteme)

A1 Pentester beschreiben

Recherchiere im Web und erstelle eine kurze Beschreibung des Berufs „Pentester".

Ablauf eines Hacks

Das Eindringen in ein Informatiksystem, um sich z. B. Zugang zu Daten zu verschaffen oder anderen Schaden anzurichten, geschieht in der Regel in drei Phasen:

1. Sammeln von Informationen (passives und aktives **Scannen**)	Zunächst wird „passiv" nach öffentlichen Informationen über das Zielsystem gesammelt (z. B. E-Mail-Adresse, Namen). Mit spezieller Software können „aktiv" weitere Informationen gesammelt werden.
2. Zugang zum Zielsystem erlangen (**Exploit**)	Mittels gesammelter Informationen können Schwachstellen ausfindig gemacht werden, um sich in das Zielsystem einzuloggen. Dabei können Passwörter gesammelt und Schadprogramme eingesetzt werden.
3. Absicht umsetzen	Wenn Hacker genügend Rechte im Zielsystem haben, können Passwörter erbeutet und das Zielsystem beschädigt werden (z. B. zum Zweck der Erpressung).

Da Hacking illegal ist, macht man sich durch aktives Scannen bereits strafbar.

to exploit: ausnutzen (von Schwachstellen)

A2 Scannen

a) Nenne Daten über Schulangehörige (Namen, E-Mailadressen), die auf der Webseite deiner Schule zu finden sind.
b) Ermittle, z. B. mit dem Browser-Plugin Wappalizer, welche Softwarepakete der Webserver deiner Schule verwendet.

Passwörter „erbeuten“

Ein großer Teil von Hacking-Aktivitäten zielt auf das Ermitteln von Zugangsdaten. Informatiksysteme müssen prüfen, ob ein Benutzer das richtige Passwort eingegeben hat. Sie speichern aber so gut wie nie die Passwörter selbst, denn dann hätte ein Hacker, der eine Liste von Passwörtern findet, sehr leichtes Spiel.
Stattdessen wird eine **Hashfunktion** verwendet. Damit wird jedem beliebigen Passwort eine Zeichenkette (der „Hashwert“) zugeordnet, die üblicherweise gleich lang ist, egal wie lang das Passwort ist:

Der deutsche Begriff für Hashfunktion ist „Streuwertfunktion“.

Passwort	Hashwert (MD5)
`Marienkäfer2000`	`d4db139e605347949a3348ace5356be9`
`Passwort123`	`fe6fa98138ffab6339e4adeee157538c`

Als Hashfunktion werden heute meist MD5 (message digest algorithm) und SHA (secure hash algorithm) verwendet.

Man kann aus einem Hashwert das ursprüngliche Passwort nicht einfach wiederherstellen. Man kann nur prüfen, ob ein eingegebenes Passwort den gleichen Hashwert produziert. Wenn Hacker eine Liste mit Hashwerten erbeuten, haben sie daher nur die Möglichkeit einer **Brute-Force-Attacke**, d. h. mögliche Passwörter nacheinander auszuprobieren. Dazu verwenden sie Listen häufig benutzter Passwörter. Ein simples Passwort kann so nach einigen Stunden ermittelt werden, für ein sicheres Passwort würde diese Methode Jahrhunderte benötigen.

A3 Passwörter und Hashwerte verknüpfen

a) Recherchiere und erkläre die Brute-Force-Attacke.
b) Recherchiere nach einer Liste mit häufig genutzten Passwörtern.
c) Erzeuge die MD5- bzw. SHA-Hashwerte einiger der unter b) gefundenen Passwörter mithilfe eines Generators.

L38043-02
MD5- und SHA-Generatoren

MERKE

Mit **Hacking** bezeichnet man das unbefugte Eindringen in Informatiksysteme. **Pentester** tun dies in friedlicher Absicht, um Sicherheitslücken in Systemen aufzudecken. Hacking geschieht in mehreren Phasen, zu denen **Scannen** und **Exploits** gehören. Um in Systeme einzudringen, werden Passwörter benötigt, die mithilfe von **Hashfunktionen** sicher gespeichert und nur durch **Brute-Force-Attacken** geknackt werden können.

AUFGABEN

1 Recherchiere und halte ein kurzes Referat zu einem der folgenden Themen bzw. Begriffe aus a), b) oder c).

a) Stelle die Geschichte eines Hacking-Angriffs vor (eine Liste bekannter Angriffe findest du hinterlegt).
b) Begriffe aus dem Bereich Hacking:
Privilege Escalation • Social Engineering • Phishing • Malware, z. B. Virus oder Trojaner • Botnetz • DDOS
c) Schutzmaßnahmen gegen Hacking-Angriffe:
Passwortrichtlinien • Single Sign On • Zwei-Faktor-Authentifizierung • Klassifizierung von Informationen in Sicherheitsstufen • Mitarbeitersensibilisierung, z. B. „Think before you click“ • Principle of least privilege • Netzwerksegmentierung • Firewall • Patch-Management (hält Software in Systemen auf dem neuesten Stand) • SIEM (Security Information and Event Management) • Pentesting

L38043-03
Liste bekannter Hacking-Angriffe

36 2.2 Kryptographie

EINSTIEG

Pakitas Eltern haben wichtige Bankdokumente digitalisiert und abgespeichert. Jedoch sorgen sie sich, dass diese Dokumente möglicherweise jemand anderes einsehen könnte oder die Dateien bei einem Hackerangriff verschwinden könnten.

- Mache Pakitas Eltern Vorschläge, wie sie ihre Dokumente schützen könnten.

ERARBEITUNG

Schutz vertraulicher Daten

Vertraulichkeit von Daten ist nicht nur Geheimdiensten vorbehalten. Jeder Mensch hat Daten, auf die nicht jeder Zugriff haben sollte, wie zum Beispiel Kontoauszüge oder Unterlagen über ärztliche Behandlungen. Die Sicherheit solcher Daten muss bei deren Aufbewahrung und Versendung gewährleistet sein.

A1 Daten schützen

Nenne mindestens fünf verschiedene Daten, die deiner Meinung nach schützenswert sind.

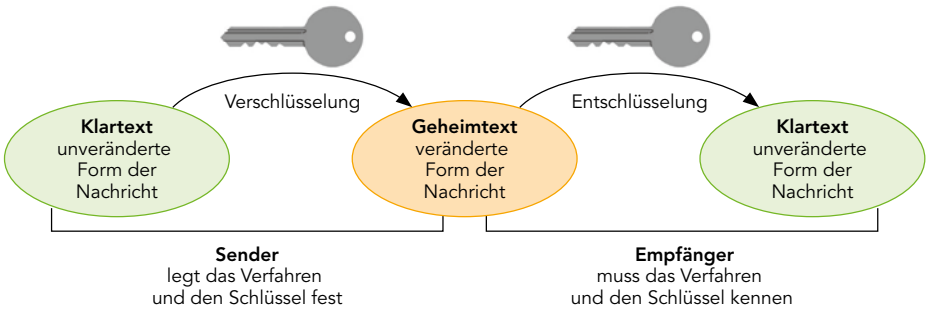
Verschlüsselung von Daten

Kryptographie stammt von den griechischen Wörtern kryptós (verborgen, geheim) und gráphein (schreiben).

Kryptographische Verfahren, die den gleichen Schlüssel zum Ver- und Entschlüsseln benutzen, nennt man „symmetrisch".

Es gibt auch asymmetrische Verfahren, die Schlüsselpaare verwenden. Dabei wird ein Teil des Paares zum Verschlüsseln, der andere zum Entschlüsseln benutzt.

Kryptographie ist eine Wissenschaft, die sich mit Verschlüsselungen beschäftigt. Um die Vertraulichkeit und Sicherheit von Daten zu gewährleisten, können Verschlüsselungsverfahren genutzt werden. Bei einem solchen Verfahren wird ein sogenannter **Klartext** in einen **Geheimtext** umgewandelt. Für die Ver- und Entschlüsselungen ist der passende **Schlüssel** notwendig.



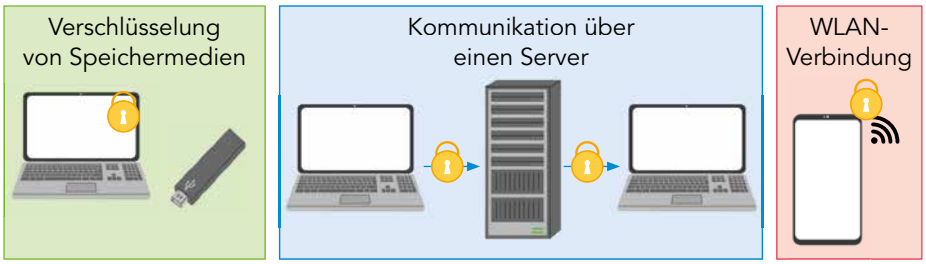
A2 Schlüssel übertragen

a) Du möchtest eine verschlüsselte Datei per E-Mail an einen Freund oder eine Freundin schicken. Erkläre Möglichkeiten, dieser Person den Schlüssel gefahrlos mitzuteilen.

b) Luca meint: „Wenn mein Weg, den Schlüssel zu übertragen, sicher ist, dann kann ich auch alle Nachrichten über diesen Weg übertragen."
Beurteile Lucas Aussage.

Anwendungen von Verschlüsselungstechnologie

Verschlüsselungen werden in vielen Situationen eingesetzt, in denen Daten digital gespeichert und übertragen werden:



Die Art der Verschlüsselung hängt dabei vom Anwendungsfall ab. Die Sicherheit einer Verschlüsselung hängt jedoch immer von der Anzahl der möglichen Schlüsselkombinationen ab. Die Nutzung des Internets würde ohne Verschlüsselung nicht funktionieren.

A3 Verschlüsselungstechnologien zuordnen

Datenträger	WLAN	Browser	E-Mail	Messenger
BitLocker (Microsoft) FileVault (Apple) VeraCrypt (Open Source)	WPA2 WPA3	SSL TLS	PGP X.509	Signal Protocol Whatsapp Protocol Skype Protocol

MERKE

Kryptographie beschäftigt sich mit Methoden, Daten zu **verschlüsseln**, um deren Vertraulichkeit zu schützen. Eine Verschlüsselung wandelt **Klartext** mithilfe eines **Schlüssels** in einen **Geheimtext** um. Die Originaldaten können nur mithilfe des passenden **Schlüssels** wiederhergestellt werden können.

AUFGABEN

1 a) Wähle dich mit einem Endgerät, z. B. deinem Handy, in ein WLAN ein. Prüfe und nenne die verwendete Verschlüsselungsmethode.
b) Recherchiere die Verbesserungen der Sicherheit bei der WPA3-Methode gegenüber der WPA2-Methode.
c) Recherchiere und erkläre die Rolle eines Radius-Servers im Zusammenhang mit der Verschlüsselung eines WLANs.

2 a) Viele Messenger-Dienste verwenden eine „Ende-zu-Ende-Verschlüsselung". Recherchiere und erkläre diese Verschlüsselungsmethode.
b) Erläutere auf Grundlage deiner Recherche, wie sich Ende-zu-Ende von der Verschlüsselung zwischen Browser und Webserver unterscheidet.

3 Bei modernen Verschlüsselungsverfahren ist das automatisierte Durchprobieren aller Schlüssel die einzig mögliche Angriffsmethode. Gehe von einem modernen PC aus, der rund 2 Milliarden Schlüssel pro Sekunde testen kann. Berechne die Zeit, die zum Testen aller Schlüssel benötigt wird:
a) Der Schlüssel besteht aus sieben Kleinbuchstaben.
b) Der Schlüssel besteht aus acht Großbuchstaben.
c) Der Schlüssel besteht aus acht Zeichen (Klein- und Großbuchstaben und die Ziffern von 0 bis 9).

38

2.3 Projekt: Einfache Geheimschriften

Verschlüsselungen werden seit Jahrtausenden eingesetzt, um vertrauliche Nachrichten zu schützen. Heutige Verfahren sind sehr komplex, aber sie beruhen in ihren Grundlagen auf historischen Verfahren. Um sich an digitale Kryptographie heranzutasten, ist es daher nützlich, sich zuerst mit älteren, einfachen Verfahren zu beschäftigen.

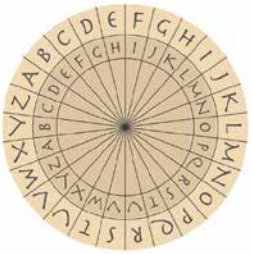
Arbeitet für die folgenden Projekte in Zweiergruppen. Probiert einige der vorgestellten Verfahren mit Papier und Bleistift aus, indem ihr jeweils eine kurze Botschaft an eure Partnerin bzw. euren Partner verschlüsselt, und die erhaltene Nachricht entschlüsselt.

Skytale

Diese Geheimschrift entstand vor ca. 2500 Jahren in der griechischen Stadt Sparta. Die Skytale ist ein achtkantiger Stab, um den früher ein Leder- oder Pergamentstreifen gewickelt wurde.
Die Nachricht wird der Länge nach auf den umwickelten Stab geschrieben. Wenn der beschriftete Streifen abgewickelt wird, ergeben die Zeichen keinen Sinn mehr.
Verwende als Ersatz für eine echte Skytale einen dicken Buntstift und anstatt eines Lederstreifens einen schmalen Streifen Papier (eine Kästchenbreite).

L38043-04
Bastelvorlage Skytale

Cäsar-Verschlüsselung



Bei dieser Methode, die z. B. von Julius Cäsar angewendet wurde, wird jedem Buchstaben ein anderer Buchstabe zugeordnet. Man schreibt unter das Alphabet für den Originaltext ein weiteres Alphabet für den Geheimtext, das um einige Stellen verschoben ist. Jeden Buchstaben des Originaltextes ersetzt man dann durch den entsprechenden Geheimbuchstaben. Beispiel:

Originalalphabet: **A**BCDEFGHIJKLMNOPQRSTUVWXYZ
Geheimalphabet: DEFGHIJKLMNOPQRSTUVWXYZ**A**BC

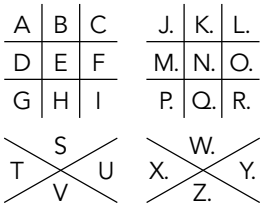
Aus „MORGEN UM ACHT“ wird der Geheimtext „PRUJHQ XP DFKW“.
Um das Verfahren zu unterstützen kann man eine Drehscheibe mit zwei Alphabeten verwenden.

L38043-05
Bastelvorlage Cäsar-Scheibe

Geheimschrift mit Zitronensaft

Wenn man Zitronensaft mit etwas Zucker mischt, erhält man eine Geheimtinte. Mit einem Federhalter (oder einem Wattestäbchen) schreibt man damit eine Botschaft auf Papier. Sobald die „Tinte“ getrocknet ist, ist sie unsichtbar.
Der Empfänger der Botschaft kann sie durch Erhitzen, z. B. im Ofen oder mit einem Bügeleisen wieder sichtbar machen.

Freimaurer-Geheimschrift



Diese Geheimschrift wurde vermutlich schon im Mittelalter von jüdischen Rabbis und den Tempelrittern, später dann von den Freimaurern benutzt. Jedem Buchstaben des Alphabets wird ein Zeichen zugeordnet, das sich aus dem abgebildeten Schema ergibt: ⌟ wird für A verwendet, ⌞ für B usw. □⌜□⌜⌝⌟<⌜□⌜ codiert beispielsweise das Wort „FREIMAURER“.

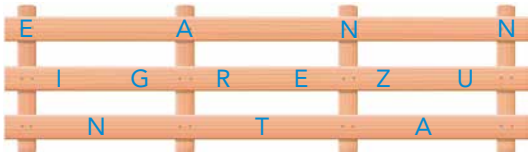
Gartenzaun

Die Buchstaben der Botschaft werden zickzackartig auf mehrere Zeilen geschrieben: der erste Buchstabe auf die oberste Zeile, der zweite auf die zweite Zeile, usw. Wenn man die unterste Zeile erreicht hat, geht es wieder nach oben. Leerzeichen werden weggelassen. Anschließend wird der Text Zeile für Zeile zusammengefasst und hintereinandergeschrieben.

Beispiel mit drei Zeilen

Originaltext: `EIN GARTENZAUN`

Zeilenweise:



→ `EANN`
→ `IGREZU`
→ `NTA`

Geheimtext: `EANNIGREZUNTA`

Internationales Signalbuch

Das internationale Signalbuch ist ein weltweit akzeptierter Standard für die Kommunikation in der Seefahrt. Es ist nicht geheim, hat aber die Eigenschaften einer Geheimschrift. Signale wie „Vorsicht, wir haben Taucher im Wasser" werden durch Buchstaben codiert. Die Buchstaben können auf verschiedene Weise übertragen werden, z. B. durch Flaggen-, Funk- oder Lichtsignale.

Stellt euch vor, dass ihr Kapitäne zweier Schiffe seid, von denen eins Schwierigkeiten hat und das andere um Hilfe bittet. Stellt eine „Unterhaltung" der beiden Kapitäne mithilfe der Signale zusammen, die ihr im Signalbuch findet.

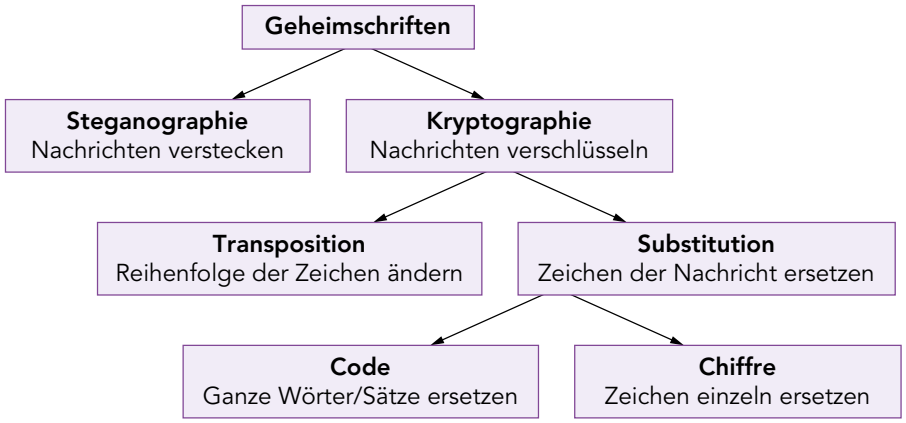
L38043-06
Internationales Signalbuch (Auszug)

Geheimschriften recherchieren

Recherchiert weitere Geheimschriften und probiert sie aus:
Atbash, die Geheimschrift Karls des Großen, das Alphabetum Kaldeorum

Geheimschriften einordnen

Geheimschriften lassen sich in folgende Struktur einordnen:



Entscheide für die von euch durchgeführten Verschlüsselungen, ob es sich um eine Methode der Steganographie, eine Transposition, einen Code oder eine Chiffre handelt.

40

2.4 Kryptoanalyse

EINSTIEG

Du hast einen geheimen Text erhalten, von dem du nicht weißt, wie er verschlüsselt wurde.

- Beschreibe Möglichkeiten, um die Verschlüsselung zu knacken und an die geheime Botschaft zu gelangen.

ERARBEITUNG

Die Häufigkeitsanalyse

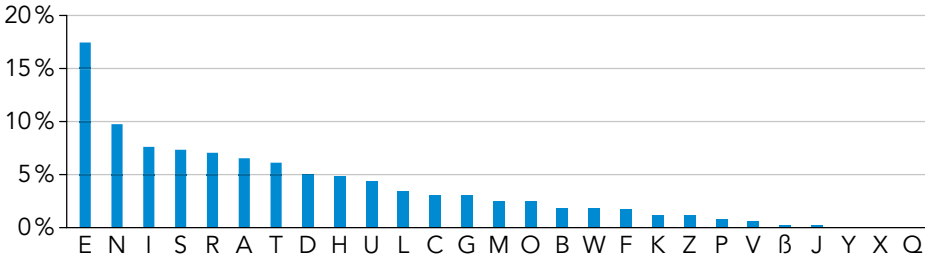
Maria Stuart

Wenn jemand Geheimnisse hat, gibt es auch Personen, die diese Geheimisse erfahren möchten: Maria Stuart, Königin von Schottland, verschlüsselte ihre Briefe, in denen sie einem Attentat auf ihre Cousine, Königin Elisabeth I. zustimmte. Diese Briefe wurden später entschlüsselt und Maria Stuart wurde zum Tode verurteilt. Geheimschriften entwickeln sich in einem Wechselspiel von Kryptographie und **Kryptoanalyse**:

Die Kryptographie entwickelt neue Verschlüsselungsmethoden.

Die Kryptoanalyse entschlüsselt neue Verschlüsselungsmethoden.

Die erste wesentliche Methode der Kryptoanalyse wurde von dem arabischen Wissenschaftler Ya'qūb al-Kindī (800–873 n. Chr.) entwickelt. Dabei untersuchte er Texte anhand ihrer Buchstabenhäufigkeit.



Buchstabenhäufigkeit in deutschen Texten

Die Buchstaben ä, ö, ü werden wie ae, oe, ue gezählt; ß als eigenes Zeichen.

Mit der **Häufigkeitsanalyse** lassen sich Geheimtexte entschlüsseln. Wenn zum Beispiel in einem Text, der mit Cäsar verschlüsselt wurde, Q der häufigste Buchstabe ist, liegt es nahe, dass Q im Original dem E entspricht.

A1 Häufigkeiten analysieren

Entschlüssele den folgenden Geheimtext mithilfe einer Häufigkeitsanalyse.
Es handelt sich dabei um eine Cäsar-Verschlüsselung – Schlüssel unbekannt.
QMPMQUBMFBM SVIKSMV QAB UIVKPUIT TMQKPBMZ ITA UIV LMVSB

Erschweren der Häufigkeitsanalyse

Die Entdeckung der Häufigkeitsanalyse machte auf einen Schlag alle Verschlüsselungsmethoden nutzlos. Eine Lösung bestand darin, häufigen Buchstaben (z. B. E) mehrere Geheimzeichen, sogenannte **Homophone** zuzuordnen. Beim Verschlüsseln wird dann jedes Mal ein Homophon zufällig ausgewählt. Man könnte beispielsweise die 26 Buchstaben auf 100 Zahlen von 0 bis 99 aufteilen. Je häufiger ein Buchstabe dabei vorkommt, umso mehr Zahlen erhält dieser.

Die „Große Chiffre" von Ludwig XIV, ein Zahlen-Code, war sicher gegen die Häufigkeitsanalyse.

A	1	10	23	45	51	87					
B	56	83									
⋮											
E	3	11	34	44	46	61	73	81	91	95	99
F	25	64									

Verschlüsselung → 10 | 64 | 25 | 73

Entschlüsselung ↓

AFFE

A2 Texte mit Homophonen verschlüsseln

Erstelle eine Tabelle, in der du jedem Buchstaben des Alphabets eine oder mehrere Zahlen zwischen 0 und 99 zuordnest. Nutze die Übersicht der Buchstabenhäufigkeit, um die Zahlen so zu verteilen, dass jede Geheimzahl etwa gleich oft im Geheimtext vorkommt.

MERKE

Die **Kryptoanalyse** entwickelt Methoden, um verschlüsselte Botschaften ohne Kenntnis des Schlüssels zu entschlüsseln.
Eine solche Methode ist die **Häufigkeitsanalyse**, mit der man über die statistische Häufigkeit von Buchstaben die Bedeutung von Geheimzeichen erraten kann.
Die Verwendung von **Homophonen** erschwert die Häufigkeitsanalyse.

AUFGABEN

1 Der folgende Geheimtext wurde mit dem Cäsar-Verfahren verschlüsselt. Knacke den Text mithilfe der Häufigkeitsanalyse:

```
ZLOYBYL, XU CWB OHYLZUBLYH OHX VYMWBYCXHYL QUL UFM BYONY,
BUNNYH GYCHY BIYWBMNY UWBNOHA UHXLY FYONY.
MJUYNYL NLUZ CWB UOZ XYL QYCXY UOMMYL GCL HIWB GYBL EUYFVYL,
OHX HOH MWBUYNT CWB, MITOMUAYH, YLMN GCWB MYFVYL.
```

2 Öffne den hinterlegten, mit Symbolen verschlüsselten Text. Darin ist die Entschlüsselung schwieriger als bei einer Cäsar-Verschlüsselung. Überlegt in Partnerarbeit, mit welchen Mitteln man auch hier die Verschlüsselung brechen kann und entschlüsselt den Text.

L38043-07
Kryptogramm für Aufgabe 2

3 Begründe, warum es nicht möglich ist, den folgenden Text mit der Häufigkeitsanalyse zu entschlüsseln:

4 Man kann die Häufigkeitsanalyse erschweren, indem man sich für jeden Buchstaben eine Zufallszahl ausdenkt. Dieser Buchstabe wird dann um die entsprechende Zahl verschoben. Der neue Buchstabe wird zur Verschlüsselung genutzt. Verschlüssele damit die Nachricht „TREFFEN AM SEE UM ZWEI" mit den folgenden Zufallszahlen: 6, 2, 9, 4, 8, 1, 7, 5, 3, 10, 2, 6, 9, 8, 4, 7, 1, 5

42 2.5 Polyalphabetische Substitution

EINSTIEG

Obwohl mit der Häufigkeitsanalyse einfache Verschlüsselungen wie Cäsar gebrochen werden konnten, wurden diese trotzdem weiter verwendet. Erst mit dem Aufkommen der Telegrafie, mit der ständig verschlüsselte Nachrichten versendet wurden, entstand der Bedarf für sicherere kryptographische Verfahren.

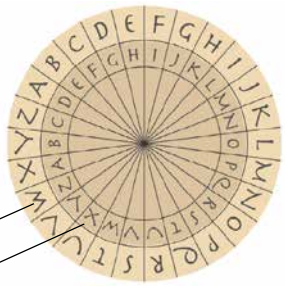
- Finde Gründe, warum man telegrafierte Botschaften verschlüsseln musste.

ERARBEITUNG

Entwicklung der polyalphabetischen Substitution

Bei einer monoalphabetischen Verschlüsselung ordnet man jedem Buchstaben aus einem **Klartextalphabet** einen Buchstaben aus dem **Geheimtextalphabet** zu.

Die dargestellte Cäsar-Scheibe dient zur Verschlüsselung von Texten mit der Verschiebung um jeweils 3 Buchstaben.



Verschlüsselungsverfahren	Jeder Buchstabe wird um einen festgelegten Wert im Alphabet nach vorne verschoben. Dadurch wird z. B. der Klartextbuchstabe A zum Geheimbuchstaben D.
Schlüssel	ein festgelegter Wert (Cäsar verwendete den Schlüssel 3.)

Das Verfahren und der Schlüssel müssen vor der Verschlüsselung festgelegt werden und sowohl Sender als auch Empfänger bekannt sein. So ist es möglich, Informationen vor unbefugten Personen zu schützen. Für „INFORMATIK“ ergibt sich im Beispiel:

Klartext	I	N	F	O	R	M	A	T	I	K
Verschlüsselung um 3 Stellen	L	Q	I	R	U	P	D	W	L	N

Schlüssel 3 bedeutet, dass jeder Buchstabe um 3 Stellen im Alphabet verschoben wird.

A1 Wie die Römer verschlüsseln

a) Verschlüssle das Wort „ROEMERLAGER“ mit dem Schlüssel 3.
b) Der folgende Satz ist mit Cäsar (Schlüssel: 4) verschlüsselt: „HMI KEPPMIV WMRH EYJ AMPHWGLAIMRNEKH“. Ermittle den Klartext.

Bei einer **polyalphabetischen** Substitution werden mehrere Geheimalphabete genutzt. Eine der ältesten Ideen ist die Alberti-Verschlüsselung. Dabei nutzt man abwechselnd zwei verschiedene Schlüssel. Beispiel für Cäsar:

Klartextalphabet	ABCD**E**FGHIJKLMNOPQR**S**TUVWXYZ
1. Verschiebung (Schlüssel: 3)	DEFG**H**IJKLMNOPQRSTUVWXYZABC
2. Verschiebung (Schlüssel: 15)	PQRSTUVWXYZABCDEFG**H**IJKLMNO

Beim ersten Buchstaben wird der erste Schlüssel verwendet, beim zweiten Buchstaben der zweite Schlüssel. Danach wird immer abgewechselt.

A2 Alberti-Verschlüsselung knacken

Durch Spionage konnte eine geheime Botschaft abgefangen werden, welche mit Alberti verschlüsselt wurde: UFJOQVUHKQIDPJ. Die Kryptologen fanden außerdem heraus, dass die Schlüssel 3 und 15 sind. Entschlüssle die Nachricht.

Verschlüsseln mit Vigenère

Blaise de Vigenère entwickelte eine weitere polyalphabetische Verschlüsselung. Dabei legt ein Schlüsselwort fest, um wie viele Stellen ein Buchstabe eines Geheimtextes zur Verschlüsselung verschoben wird. Um einen Text mit dem **Vigenère-Verfahren** zu verschlüsseln, muss das Codewort zunächst wiederholt unter den Text geschrieben werden. Buchstabe für Buchstabe verschlüsselt man dann den Text mithilfe des nachfolgend rechts abgebildeten Vigenère-Quadrats.

L38043-08
Vigenère – Schritt für Schritt und Vigenère-Quadrat

Klartext	EINVERSTANDEN
Schlüsselwort	CODECODECODEC
Geheimtext	GWQZGFVXCBGIP

A3 Vigenère-Chiffre ausprobieren

Verschlüsselt jeweils eine Botschaft mithilfe des Vigenère-Verfahrens. Nutzt für die Verschlüsselung ein „Vigenère-Quadrat". Übergebt eurer Partnerin bzw. eurem Partner den Geheimtext und das Schlüsselwort, um die Botschaft zu entschlüsseln.

Varianten der Vigenère-Methode

Die Autokey-Verschlüsselung wurde ebenfalls von Vigenère entwickelt. Statt das Schlüsselwort zu wiederholen, wird es bei diesem Verschlüsselungsverfahren nur einmal aufgeschrieben und um den Klartext ergänzt.

Klartext	E	I	N	V	E	R	S	T	A	N	D	E	N
Schlüsselwort	C	O	D	E	**E**	**I**	**N**	**V**	**E**	**R**	**S**	**T**	**A**
Geheimtext				Z	I	Z	F		E	E		X	

L38043-09
Autokey-Chiffre

A4 Autokey-Verschlüsselung nutzen

a) Nutze das Vigenère-Quadrat, um den vollständigen Geheimtext anzugeben.
b) Verschlüssle den Klartext TREFFEN UM DREI mit der Autokey-Verschlüsselung. Nutze ein selbst gewähltes Schlüsselwort.

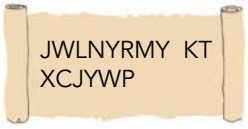
MERKE

Bei einer **monoalphabetischen** Verschlüsselung ordnet man jedem Klartextbuchstaben aus einem Klartextalphabet einen festen Buchstaben aus dem Geheimtextalphabeten zu. Für **polyalphabetische** Verschlüsselungen (wie z. B. der **Vigenère-Verschlüsselung**) werden mehrere Geheimtextalphabete verwendet.

AUFGABEN

1 Begründe, warum man einen mit Vigenère verschlüsselten Text nicht wie bei der Cäsar-Verschlüsselung mit der Häufigkeitsanalyse knacken kann.

2 Die folgende Botschaft konnte abgefangen werden. Eine Analyse ergab das Schlüsselwort SCHLOSS. Es ist jedoch unklar, welche Vigenère-Methode verwendet wurde. Entschlüssele die Nachricht und nenne die genutzte Vigenère-Methode.



Vigenère oder Autokey

44 2.6 Der Kasiski-Test

EINSTIEG

Betrachte die folgende Geheimbotschaft.

```
VHVS SP QUCE MRVBV BBB VHVS URQ
GIBDU GRNICJ QUCE RVUAX SSR
```

- Kannst du ein Muster erkennen?

ERARBEITUNG

Brechen der Vigenère-Verschlüsselung

Die Methode von Vigenère wurde die unknackbare Chiffre genannt. Etwa 200 Jahre lang galt sie als sicher. Doch im 19. Jahrhundert entwickelten der englische Mathematiker Charles Babbage und der preußische Kryptoanalytiker Friedrich Wilhelm Kasiski unabhängig voneinander ein Verfahren, mit dem sich Vigenères Verschlüsselung unter bestimmten Voraussetzungen sogar recht leicht knacken lässt. Da Babbage seine Entdeckung geheim halten musste, wurde die Methode „Kasiski-Test" genannt.

le chiffre indechiffrable (franz.): die unknackbare Geheimschrift

Charles Babbage (1791–1871) erfand neben seinen Beiträgen zur Kryptographie auch den ersten programmierbaren Computer, die Analytical Engine.

A1 Vigenère-Kryptogramm entschlüsseln

Mit der Methode von Babbage bzw. Kasiski ermittelt man die Länge des Schlüsselwortes eines mit Vigenère verschlüsselten Textes. Nimm an, dass du bereits weißt, dass für den folgenden Text ein Schlüsselwort mit zwei Buchstaben benutzt wurde – der erste Buchstabe für die blauen, der zweite für die roten Buchstaben:

```
LNM LMIISSJV XQSL KZJQ BMW SFVS ANM JZWIYMS
ANM KTNMMMS DTZGMN ENM SIJKMBQQHPJ AHPFBYMS
SJQS UJVXKM SFVS ANM BQXAJV PMNV OIJOJZ JZXKMQJAXMS
MX JQMNJJB IIGMN LNM LMIISSJV XQSL KZJQ
```

a) Erkläre, wie du die Häufigkeitsanalyse einsetzen kannst, um Informationen über die beiden verwendeten Alphabetverschiebungen zu erhalten.

b) Entschlüssle die Botschaft und gibt das Schlüsselwort an.

Der Kasiski-Test

Mit dem **Kasiki-Test** kann die Länge des Schlüsselwortes der Vigenère-Verschlüsselung ermittelt werden. Dies beruht auf der Wiederholung häufiger Wörter, wie „der", „die" oder „das". Bei einem längeren Text ist es wahrscheinlich, dass diese an einigen Stellen gleich verschlüsselt werden, da sich das Schlüsselwort an anderer Stelle wiederholt. Zum Beispiel wiederholt sich die Verschlüsselung des Wortes „ich" nach 12, die des Wortes „Was" nach 15 Buchstaben, weil das Schlüsselwort in beiden Fällen die gleiche Position hat:

```
Klartext:     ICH DENK AN WAS ICH WILL SOWIE WAS MICH BEGLUECKT
Schlüsselwort: MIT MITM IT MIT MIT MITM ITMIT MIT MITM ITMITMITM
Geheimtext:   UKA PMGW IG IIL UKA IQEX AHIQX IIL YQVT JXSTNQKDF
              12 Buchstaben   15 Buchstaben
```

Aus der Analyse des Geheimtextes kann man schließen, dass das Schlüsselwort 3 Buchstaben lang ist. Die Wiederholung kann nur entstehen, wenn sich das Schlüsselwort in beiden Fällen an der gleichen Stelle wiederholt. Das kann nur der Fall sein, wenn sich sowohl 12 wie 15 durch die Länge des Schlüsselwortes teilen lassen.

Allgemein ist das Vorgehen wie folgt:

① Man sucht mindestens zwei Wiederholungen im Geheimtext, die jeweils mindestens drei Buchstaben lang sind.

② Man zählt, nach wie vielen Buchstaben sich diese Wörter wiederholen.

③ Der größte gemeinsame Teiler (ggT) dieser Abstände ist vermutlich die Länge des Schlüsselwortes (auch ein kleinerer Teiler ist möglich).

④ Die Buchstaben des Geheimtextes teilt man in so viele Gruppen ein, wie das Schlüsselwort Buchstaben hat. Für jede dieser Gruppen wird der Buchstabe ermittelt, der am wahrscheinlichsten dem E entspricht.

⑤ Die Bedeutung der restlichen Geheimbuchstaben ergibt sich, da jede der Buchstabengruppen mit einer Alphabetverschiebung verschlüsselt wurde.

A2 Den Kasiki-Test anwenden

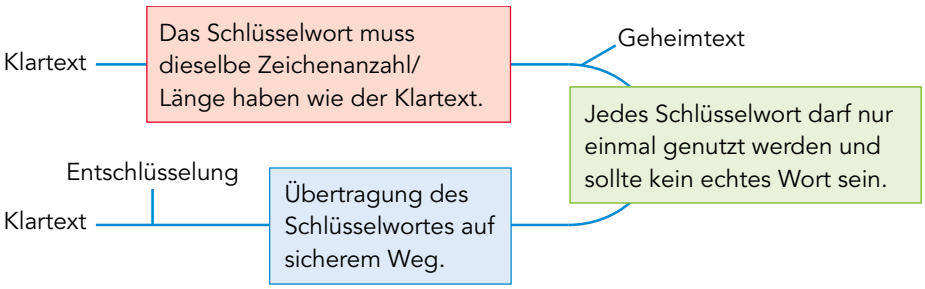
Öffne den hinterlegten, mit Vigenère verschlüsselten Text. Entschlüssle ihn mithilfe des Kasiski-Tests.

L38043-10
Geheimtext und Hilfestellung für A2

One-Time-Pad (Vernam-Chiffre)

1919 patentierte der Amerikaner Gilbert Vernam eine kryptographische Methode, von der mathematisch nachgewiesen ist, dass sie unmöglich geknackt werden kann. Man verwendet ein Schlüsselwort, das genauso lang ist wie die Botschaft selbst und aus zufällig gewählten Buchstaben besteht.

One-Time-Pads wurden im 20. Jahrhundert von Diplomaten und Geheimdiensten eingesetzt.



MERKE

Mit dem **Kasiski-Test** kann man die Länge des Schlüsselwortes eines mit der Vigenère-Methode verschlüsselten Textes ermitteln. Basierend darauf kann man den Text durch mehrmalige Häufigkeitsanalyse entschlüsseln.
Ein **One-Time-Pad** ist ein Schlüsselwort, das aus zufälligen Buchstaben besteht, genauso lang ist wie die Botschaft und nur einmal verwendet wird.

AUFGABEN

1 Ein weiteres Verfahren zum Brechen der Vigenère-Verschlüsselung ist die Auto-Korrelation. Informiere dich auf der hinterlegten Website über diese Methode und erstelle einen kurzen Steckbrief.

2 Das von Vernam entwickelte One-Time-Pad ist zwar hundertprozentig sicher, aber das Verfahren hat auch gravierende Nachteile. Recherchiere die Verwendung von One-Time-Pads und erläutere entsprechende Nachteile.

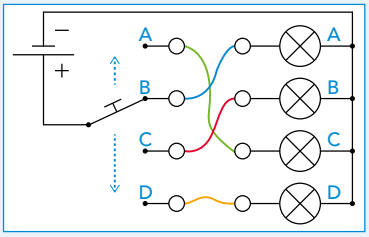
L38043-11
Aufgabe 1

46 2.7 Die Enigma

EINSTIEG

Rechts ist eine elektrische Schaltung abgebildet.

- Was bedeuten die einzelnen Symbole?
- Wie fließt hier der Strom?
- Nimm an, dass man die farbigen Drähte in der Mitte der Schaltung unterschiedlich verknüpfen kann. Wie könnte man die Schaltung für eine Verschlüsselung einsetzen?



ERARBEITUNG

Die Entwicklung maschineller Verschlüsselung

Fortschritte in der Kryptoanalyse erforderten immer bessere Verschlüsselungsmethoden. Doch schon Vigenères Chiffre war mit Papier und Bleistift so zeitraubend, dass sie kaum in der Praxis eingesetzt wurde – und auch diese Methode erwies sich als unsicher.
1918 entwickelte Arthur Scherbius die **Enigma**. Die Enigma ist eine komplexe Chiffrenmaschine zur Verschlüsselung von Nachrichten. Im Gegensatz zu früheren Verschlüsselungen nutzt die Enigma Rotoren, die mit Strom angetrieben wurden. Sie wurde von der Wehrmacht im Zweiten Weltkrieg eingesetzt. Die spannende Geschichte ihrer Entschlüsselung und ihr Name machten sie zur vielleicht bekanntesten Chiffriermaschine.

A1 Schlüssel täglich wechseln

Die deutsche Wehrmacht nutzte für die Entschlüsselung von Enigma-Nachrichten täglich geänderte Schlüssel. Erkläre die Bedeutung dieser Änderungen.

Der Aufbau

Die Engima besteht aus einer Tastatur, einer Reihe von Walzen (Rotorwalzen), einem Steckbrett und einer Anzeigetafel. Diese Elemente ermöglichen die Verschlüsselung.

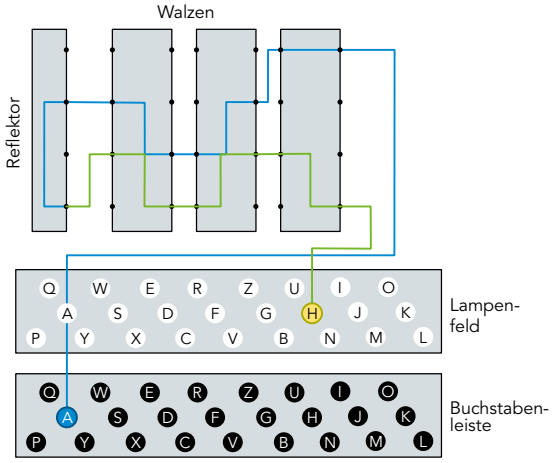
A2 Aufbau Enigma

a) Recherchiere die Funktion der einzelnen Bestandteile einer Enigma, die in der Abbildung zu sehen sind.

b) In der Abbildung sind die Reflektoren nicht zu sehen. Recherchiere deren Funktion in der Enigma.

Die Verschlüsselungstechnik

Jede Walze hat 26 Metallkontakte auf beiden Seiten, einen pro Buchstaben des Alphabets. Im Inneren sind diese Kontakte mit Drähten verbunden. Wenn ein Buchstabe auf der Tastatur gedrückt wird, wird der Strom durch die drei Walzen geleitet. Der Reflektor hinter der dritten Walze hat ebenfalls 26 Kontakte, aber nur auf einer Seite, von denen je zwei miteinander verdrahtet sind. Er leitet den Strom wieder zurück durch die drei Walzen und dann an das Lampenfeld, wo der chiffrierte Buchstabe aufleuchtet.



Damit die Buchstaben nicht immer gleich verschlüsselt werden, dreht sich die erste Walze nach jedem eingetippten Buchstaben eine Position weiter. Wenn die erste Walze sich 26-mal gedreht hat, dreht sich die zweite eine Position weiter, und wenn die sich einmal ganz herumgedreht hat, die dritte. So erzeugt die Enigma eine polyalphabetische Chiffre. Ein großer Vorteil der Enigma ist, dass sie auf die gleiche Art auch entschlüsselt. Wenn man einen Geheimtext eintippt, erscheint auf dem Lampenfeld der Originaltext.

Entschlüsselung der Enigma

Obwohl die Enigma zunächst völlig sicher zu sein schien, gelang es dem polnischen Mathematiker Marian Rejewski in den 1930er Jahren, die damalige Version der Enigma zu knacken. Die Enigma wurde jedoch verbessert, und mit dem deutschen Angriff auf Polen konnte er seine Arbeit nicht fortsetzen. Seine Forschungsergebnisse wurden aber an die Alliierten weitergegeben, so dass es dem Briten Alan Turing und seinen Mitarbeitern gelang, auch die späteren Versionen der Enigma zu entschlüsseln und so entscheidend zu einem früheren Ende des Zweiten Weltkriegs beizutragen.

Alan Turing (1902–1954) leistete wichtige Beiträge zur Entwicklung moderner Computer. Er gilt als einer der „Väter" der Informatik.

MERKE

Die **Enigma** ist eine elektrische Chiffriermaschine. Auf ihrer **Tastatur** wird der Originaltext oder der Geheimtext eingetippt. Die Buchstaben werden elektrisch mithilfe von drehbaren **Walzen** und einem **Reflektor** in andere Buchstaben umgewandelt und können auf einem **Lampenfeld** abgelesen werden.

AUFGABEN

1 Arbeitet im Zweierteam. Hinterlegt findet ihr eine Bastelvorlage (mit Anleitung), auf der Walzen und Reflektoren der Enigma als Papierstreifen abgedruckt sind. Verschlüsselt damit jeweils eine Botschaft und lasst sie von der anderen Person entschlüsseln.

2 Das Knacken der Verschlüsselung der Enigma hatte einen entscheidenden Einfluss auf den Verlauf des Zweiten Weltkrieges.
Recherchiere wie es Alan Turing und seinem Team gelang, das Verschlüsselungsverfahren der Enigma zu entschlüsseln. Fasse deine Ergebnisse zusammen.

L38043-12
Aufgabe 1

48 2.8 Computergestützte Verschlüsselung

EINSTIEG

Neben der Enigma wurden viele weitere Verschlüsselungsmaschinen gebaut. Eine davon ist die 1943 von Siemens & Halske entwickelte T43 mit dem englischen Codenamen „Thrasher". Sie benutzte Lochstreifen für binär codierte Nachrichten und Schlüssel. Als Schlüssel war theoretisch ein One-Time-Pad möglich, womit die Verschlüsselung unmöglich zu brechen wäre.

- Recherchiere die Geschichte dieser Maschine und erkläre die Verschlüsselungsmethode kurz.

ERARBEITUNG

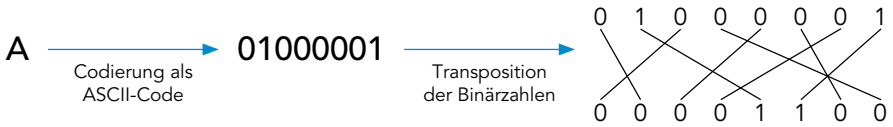
Binärzahlen verschlüsseln

Ein Computer verarbeitet und speichert Daten mithilfe von Binärzahlen. Für einen Buchstaben braucht man im ASCII-Code z. B. eine achtstellige Binärzahl (acht Bits bzw. ein Byte). Moderne Verschlüsselungsmethoden verarbeiten Binärzahlen und wenden dabei Transpositionen und Substitutionen an.

Transposition = Änderung der Reihenfolge der einzelnen Bits

Substitution = Ersetzen von Bits durch andere

Eine Transposition ist mathematisch eine sogenannte **Permutation**. Das folgende Beispiel zeigt die Permutation (2, 5, 1, 8, 3, 7, 4, 6) für eine achtstellige Bitfolge:



A1 Permutationen durchführen

a) Beschreibe für obiges Beispiel, wie die Permutation durchgeführt wird.

b) Bilde die Permutation (2, 4, 6, 8, 1, 3, 5, 7) der Binärzahl 1 1 0 0 1 1 0 0.

XOR: exclusive or (ausschließendes oder bzw. „entweder – oder")

a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

Für die Substitution von Binärzahlen wird in computergestützten Verschlüsselungen meist eine weitere Binärzahl als Schlüssel verwendet. Die zu verschlüsselnde Zahl und der Schlüssel werden mithilfe der **XOR-Operation** verrechnet. a XOR b ist 1, wenn entweder a oder b den Wert 1 hat, ansonsten ist a XOR b = 1 (siehe Tabelle).

Verschlüsselung

Zahl	1	1	0	0	1	0	0	1
Schlüssel	1	0	1	0	1	0	1	0
	↓	XOR						
Geheimtext	0	1	1	0	0	0	1	1

Entschlüsselung

Zahl	1	1	0	0	1	0	0	1
	↑	XOR						
Schlüssel	1	0	1	0	1	0	1	0
Geheimtext	0	1	1	0	0	0	1	1

Man bildet für jede Stelle der zu verschlüsselnden Zahl und des Schlüssels das XOR. Der Schlüssel kann zufällig generiert oder eine vom Benutzer bestimmte Zahl sein.

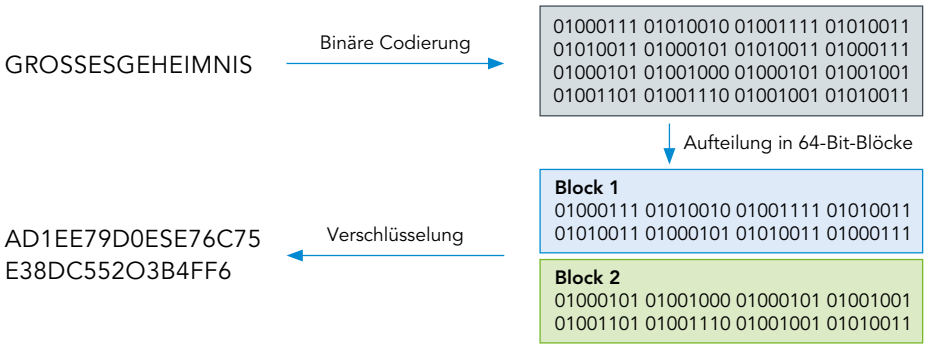
A2 Binäre Transposition und Substitution anwenden

a) Verschlüssle die Zahl 1 1 0 0 1 1 0 0 mit XOR und dem Schlüssel 1 0 0 1 0 0 1 0.

b) Entschlüssle 1 0 1 1 1 0 0 0 mit XOR und dem Schlüssel 1 0 0 1 0 0 1 0.

Blockchiffren

Moderne Verschlüsselungsverfahren sind Blockchiffren. Mit ihnen verschlüsselt man nicht jeden Buchstaben einzeln, sondern mehrere Buchstaben gemeinsam. Die Grundlage für heutige Blockchiffren war der Data-Encryption-Standard (DES). Dieser nutzte zur Verschlüsselung einen 64 Bit langen Schlüssel. Dabei wird ein Text in 64-Bit-Blöcke eingeteilt – wenn ein Buchstabe 8 Bits benötigt, sind dies jeweils 8 Buchstaben.



Durch die immer stärker werdende Rechenleistung kann diese Verschlüsselung mit der Brute-Force-Methode gebrochen werden. Daher wird heute das **Advanced Encryption Standard (AES)** verwendet. AES ist heute die am häufigsten verwendete Verschlüsselungsmethode für digitale Daten.

A3 AES-Verfahren recherchieren

a) Recherchiere Merkmale dieses Verfahrens. Gehe dabei auch auf die Schlüssellänge ein.
b) Finde heraus, in welchen Bereichen AES eingesetzt wird.

MERKE

Mit einer **Permutation** kann man binär codierte Nachrichten durch eine Transposition verschlüsseln. Eine Substitution kann mithilfe eine Schlüssels und der **XOR-Operation** durchgeführt werden.
Für eine **Blockchiffre** wird eine binär codierte Nachricht in Blöcke fester Länge (z. B. 64 Bit) geteilt, die dann jeweils als Block verschlüsselt werden. Der aktuelle Standard zur Verschlüsselungen heißt **Advanced Encryption Standard** (**AES**).

AUFGABEN

1 Mithilfe von Permutation und Substitution lässt sich beispielhaft folgende Verschlüsselungsmethode konstruieren.
① Teile den Originaltext, der binär codiert ist, in 16-Bit-Blöcke ein. Falls für den letzten Block nicht genügend Bits übrig sind, fülle ihn mit Nullen auf.
② Wende auf jeden Block eine immer gleiche Permutation an:
(4, 14, 10, 2, 16, 6, 7, 3, 1, 15, 13, 5, 8, 12, 9, 11)
③ Codiere ein Schlüsselwort als Binärzahl und nutze diesen als Schlüssel für die XOR-Operation.

a) Stelle die Botschaft „KIEL" mit dem ASCII-Code als Binärzahl dar.
b) Verschlüssle sie mit der beschriebenen Methode und dem Schlüssel „IF".
c) Entschlüssle folgenden Geheimtext mit dem Schlüssel „BV", indem du die Substitution umkehrst und anschließend die Permutation rückgängig machst:
0100 0010 0110 0001 0100 0110 0100 0001

D	68	0100	0100
E	69	0100	0101
F	70	0100	0110
G	71	0100	0111
H	72	0100	1000
I	73	0100	1001
J	74	0100	1010
K	75	0100	1011
L	76	0100	1100

ASCII (Ausschnitt)

50

2.9 Üben und Vertiefen

1 Verschlüsselungen gewährleisten die Sicherheit von Daten und sind heute unerlässlich.

a) Erkläre den Unterschied zwischen einer monoalphabetischen und einer polyalphabetischen Verschlüsselung.
b) Nenne und erkläre jeweils ein Beispiel.

a) Gib die binäre Darstellung der Buchstabenfolge „IF“ (codiert mit ASCII) an.
b) Wende die Permutation (16, 1, 15, 2, 14, 3, 13, 4, 12, 5, 11, 6, 10, 7, 9, 8) auf die Binärzahl aus Aufgabe a) an.
c) Nach der Transposition wird die XOR-Operation angewendet. Erkläre den Vorteil dieses Vorgehens.

2 Hackerangriffe und deren Gefahren sind in den letzten Jahren immer häufiger geworden.

Silvia hat folgende E-Mail von ihrer Bank erhalten. Beurteile die Situation und gib Silvia Ratschläge.

Absender: IhreBank@bankhaus.de
Betreff: Irrtum zu Ihren Gunsten!

Sehr geehrte Frau Mustermann,

bei unserer letzten Abrechnung ist uns ein Fehler unterlaufen. Als Entschädigung erhalten Sie von uns eine großzügige Ausgleichszahlung. Bitte klicken Sie dazu auf den folgenden Link und melden Sie sich mit Ihren Anmeldedaten an.

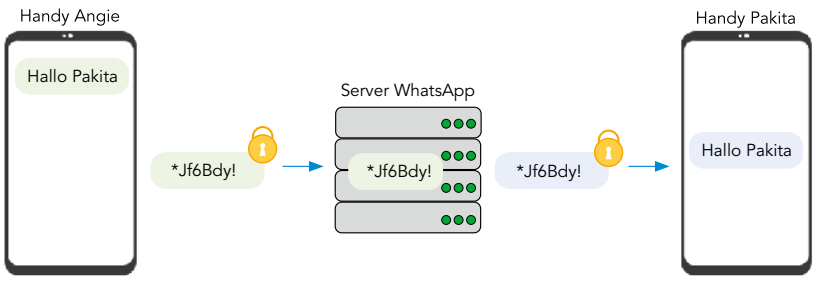
IhreBank.de/Anmeldung

Wir entschuldigen uns für das Problem.

Mit freundlichen Grüßen
Ihre Bank

a) Erläutere die Gemeinsamkeiten und Unterschiede zwischen Hackern und Pentestern.
b) Erläutere, wie ein Hacker mithilfe einer Liste von Hash-Werten Passwörter erbeuten kann.
c) Liste die Phasen eines Hacks auf und erläutere diese kurz.

3 Die Ende-zu-Ende-Verschlüsselung ist eines der wichtigsten Verschlüsselungsverfahren im Bereich Social Media.



a) Erkläre die obige Grafik und gehe dabei auf die einzelnen Schritte ein.
b) Recherchiere die Datenschutzfunktionen von WhatsApp und erstelle eine Übersicht.

a) Neben der Ende-zu-Ende-Verschlüsselung findet man auch die Punkt-zu-Punkt-Verschlüsselung. Informiere dich mit geeigneten Quellen über diese Verschlüsselungsmethode.
b) Beurteile die Sicherheit der Punkt-zu-Punkt-Verschlüsselung gegenüber der Ende-zu-Ende-Verschlüsselung.

4 Vergleiche das Brute-Force-Verfahren mit der Häufigkeitsanalyse. Erläutere, in welchen Situationen welches Verfahren verwendet wird.

5 a) Nutze die Vigenère-Verschlüsselung zur Verschlüsselung des Klartextes „ZAHLENSCHLOSS" mit dem Schlüssel „CODE".
b) Die geheime Botschaft „IJIGOCIAIV" wurde abgefangen. Durch Spionage konnte herausgefunden werden, dass der Schlüssel „TEIG" lautet. Entschlüssle die abgefangene Nachricht.
c) Begründe die höhere Sicherheit im Vergleich zum Cäsar-Verfahren.

6 Valentina und Cem einigen sich darauf, ihre Kommunikation mit Morsezeichen zu verschlüsseln, indem sie einfach lange und kurze Signale vertauschen. So werden zum Beispiel U (..-) und G (--.) miteinander vertauscht.
a) Entschlüssele die Nachricht ONGDTEEK.
b) Begründe, dass die Gesamtzahl der für eine Nachricht zu sendenden Signale (kurze oder lange Impulse) durch diese Verschlüsselung gleich bleibt.
c) Begründe, dass durch die Verschlüsselung in der Regel mehr Zeit benötigt wird, um die Nachrichten zu versenden.
d) Begründe, warum diese Verschlüsselung nicht immer durchführbar ist.

7 a) Verschlüssele mit deiner Enigma eine beliebige Nachricht.
b) Tausche deinen Geheimtext mit einer anderen Person aus und entschlüssle deren Geheimtext.

8 a) Erläutere, warum ein längeres Schlüsselwort die Vigenère-Methode sicherer macht.
b) Beschreibe, wie du ein beliebiges Buch einsetzen könntest, um eine Botschaft mit der Vigenère-Methode zu verschlüsseln. Dabei soll nur jemand, der über das gleiche Buch verfügt, die Botschaft wieder entschlüsseln können. Nenne den Schlüssel.
c) Recherchiere, warum man ein One-Time-Pad nur ein einziges Mal benutzen darf, um eine Entschlüsselung unmöglich zu machen.

9 Das Advanced Encryption Standard (AES) ist ein Verschlüsselungsverfahren, das zur sicheren Übertragung von Daten verwendet wird. Es basiert auf einer symmetrischen Blockchiffre. Sowohl der Sender als auch der Empfänger verwenden denselben Schlüssel. Das AES-Verfahren verwendet eine Netzwerkstruktur, bei der die Daten in Blöcke von 128 Bit aufgeteilt werden. Diese Blöcke werden dann durch eine Reihe von Operationen verschlüsselt. AES bietet verschiedene Schlüssellängen, nämlich 128, 192 und 256 Bit.
a) Recherchiere, wie viele Schlüsselkombinationen es bei AES mit einer Schlüssellänge von 128 (192, 256) Bit gibt. Gib die Ergebnisse als Potenzen an.
b) Mit welcher dir bekannten Methoden könnte man einen Schlüssel der Länge 128 Bit knacken?

10 Recherchiere und erläutere die Bedeutung von „Security through Obscurity". Nenne und erkläre zudem kurz das passende Gegenkonzept.

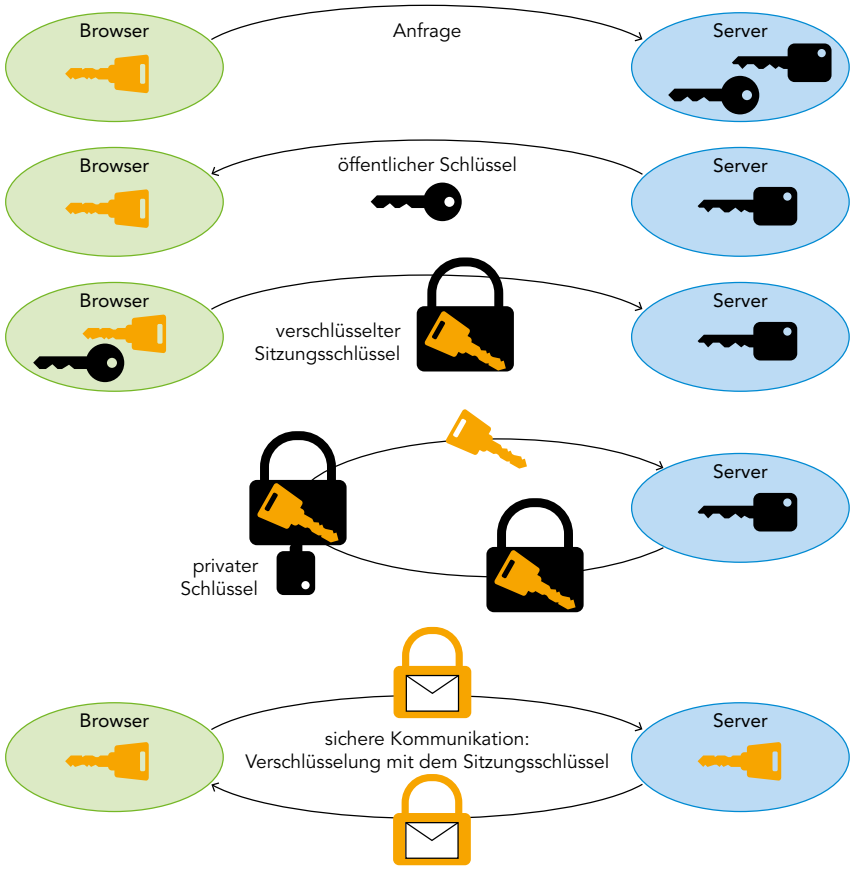
52 2.9 Üben und Vertiefen

11 Neben der symmetrischen Verschlüsselung gibt es auch die Möglichkeit der asymmetrischen Verschlüsselung. Der große Unterschied dabei ist, dass für die Ver- und Entschlüsselung nicht der gleiche Schlüssel genutzt wird.

a) Recherchiere den Begriff der asymmetrischen Verschlüsselung und erkläre diesen. Erstelle zur Veranschaulichung ein entsprechendes Schaubild.

b) Asymmetrische Verschlüsselungen kommen insbesondere bei der Verschlüsselung im Browser per HTTPS zum Einsatz. Dieses Verfahren wird durch das folgende Beispiel dargestellt. Erkläre das in der Grafik dargestellte Verfahren des Schlüsseltausches. Gehe hierzu auf alle gezeigten Schritte ein und achte jeweils auf die Rollen der privaten und öffentlichen Schlüssel.

HTTPS: Hypertext Transfer Protocol Secure

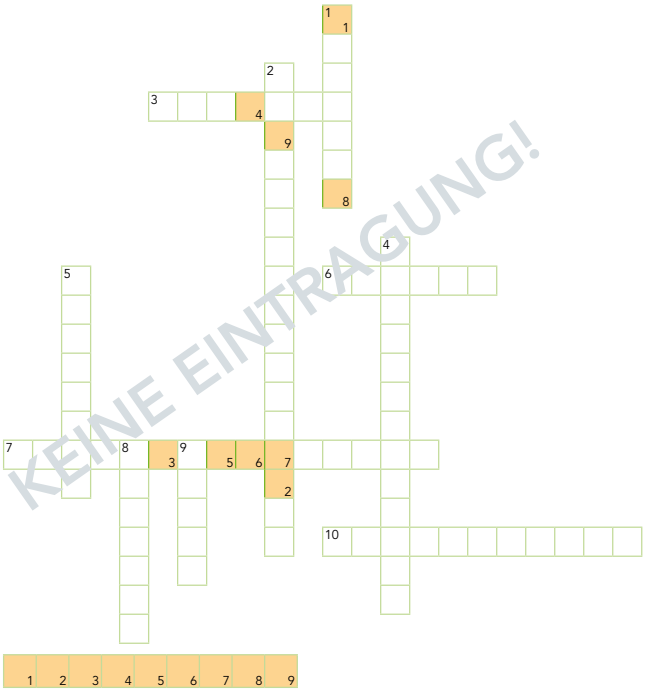


12 Der Geheimtext „MNHOREGENAX“ ist durch das Cäsar-Verfahren entstanden – Schlüssel unbekannt. Knacke die Verschlüsselung durch die Brute-Force-Methode.

13 Der folgende Binärcode konnte abgefangen werden: 00001010. Er wurde mit der folgenden Permutation verschlüsselt: (3, 7, 4, 8, 1, 5, 2, 6). Mache die Permutation rückgängig und finde den zugehörigen Klartextbuchstaben (ASCII).

Das große Info-Quiz!

Öffne die hinterlegte Datei und löse das Rätsel.



L38043-13
Info-Quiz

1. Mit welcher Methode wurden vor 2500 Jahren in Griechenland Botschaften verschlüsselt?
2. Vigenère ist eine ... Substitution.
3. In dieser Phase des Hackings dringen Angreifer in ein Informatiksystem ein.
4. Die … entwickelt Methoden, um Verschlüsselungen zu brechen.
5. Passwörter für Informatiksysteme werden als ... gespeichert.
6. Erfinder des One-Time-Pad
7. Umwandlung von Klartext in Geheimtext
8. Mit einer ... werden einzelne Zeichen einer Nachricht ersetzt.
9. Mit dem Kasiski-Test ermittelt man die ... des Schlüsselwortes.
10. Einen verschlüsselten Text nennt man auch ...

1 a) Erläutere die Bedeutung einer Hashfunktion und des Hashwertes.
b) Erkläre, warum man keine zu einfachen Passwörter nutzen sollte.

2 a) Verschlüssle die Botschaft „Ich habe es geschafft“ mit einer Cäsar-Verschlüsselung um 7 Stellen.
b) Verschlüssle die gleiche Botschaft mit der Vigenère-Chiffre und dem Schlüsselwort „INFO“.

3 a) Erläutere, wie du mit dem Kasiski-Test eine mit Vigenère verschlüsselte Botschaft entschlüsseln kannst.
b) Erläutere, was ein One-Time-Pad ist und warum diese Chiffriermethode nicht geknackt werden kann.

4 Erläutere Blockchiffre, Permutation und XOR-Operation an einem Beispiel.

Ich kann …	In Aufgabe	Hilfe
den Begriff Hashfunktion und die Bedeutung von sicheren Passwörtern erläutern.	1	2.1
Substitutionsverfahren als Möglichkeit der Verschlüsselung verwenden.	2	2.5
verschiedene Verschlüsselungsverfahren unter Berücksichtigung von ausgewählten Sicherheitsaspekten beurteilen.	3	2.6
computergestützte Verschlüsselungsverfahren an Beispielen erläutern.	4	2.8

54

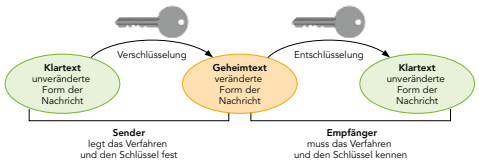
2.11 Alles im Blick

Bedrohung für die Sicherheit durch Hacking ➥ 2.1

Das illegale Eindringen in Informatiksysteme wird als Hacking bezeichnet. Dieser Prozess kann in verschiedenen Phasen verlaufen. Häufig zielen Hacker auf Passwörter ab. Durch das Erbeuten von Hashwerten und eine Brute-Force-Attacke können Passwörter ermittelt werden.

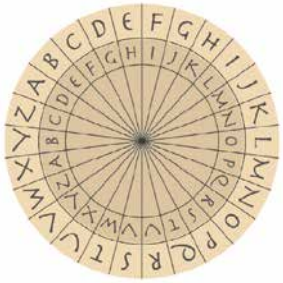
Verschlüsselung von Daten ➥ 2.2

Der Sender verschlüsselt eine Nachricht mit dem Ziel, dass nur der Empfänger die Nachricht versteht. Dabei wird der Klartext einer Nachricht in einen Geheimtext verschlüsselt. Dadurch bleiben Daten geschützt.



Verschlüsselungsmethoden ➥ 2.5, 2.7, 2.8

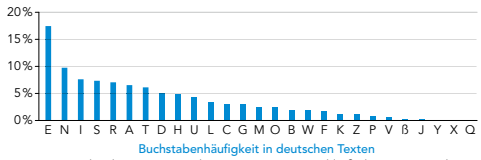
Verschlüsselungsmethoden wie das Cäsar- oder Vigenère-Verfahren werden seit vielen Jahrhunderten verwendet. Im Laufe der Zeit entwickelten sich immer komplexere Verschlüsselungsmethoden, wie die Enigma oder Blockchiffren. Man unterscheides zwischen mono- und polyalphabetischen Verschlüsselungsmethoden.



I	N	F	O	R	M	A	T	I	K
L	Q	I	R	U	P	D	W	L	N

Kryptoanalyse ➥ 2.6

Mit der Häufigkeitsanalyse und dem Kasiki-Test können mono- und polyalphabetische Verschlüsselungen geknackt werden.



Buchstabenhäufigkeit in deutschen Texten
Die Buchstaben ä, ö, ü werden wie ae, oe, ue gezählt; ß als eigenes Zeichen.

FACHBEGRIFFE

Hier findest du die wichtigsten Begriffe aus diesem Kapitel:

Hacker	Kryptogramm	Kryptoanalyse
Pentester	monoalphabetisch	Kasiki-Test
Brute-Force	polyalphabetisch	One-Time-Pad
Kryptographie	Vigenère	Enigma
Blockchiffre	Permutation	XOR

Ausblick: Das erwartet Sie in den weiteren Kapiteln des Buches

Eintauchen in die Welt des textbasierten Programmierens

Das textbasierte Programmieren stellt einen wesentlichen neuen Lehrplaninhalt dar und ist häufig eine Herausforderung für Schülerinnen und Schüler. Unser Schulbuch ist darauf ausgelegt, die Grundlagen des textbasierten Programmierens in Python zu vermitteln und Schritt-für-Schritt zu immer weiteren komplexeren Programmen zu gelangen. Durch das Zurückgreifen auf Scratch-Kenntnisse wird ein leichterer Übergang geschaffen.

Mit Informatik 9/10 werden Ihre Schülerinnen und Schüler:

- die Begriffe Syntax und Semantik in Python verstehen und anwenden
- ein Verständnis über Bibliotheken und deren Bedeutung entwickeln
- Quelltexte gezielt modifizieren und richtig ergänzen
- Schleifen und Funktionen erstellen und anwenden
- Variablen, Parameter und Verzweigungen einsetzen

Um die gelernten Programmierkenntnisse anzuwenden steht ein Projektkapitel zur Verfügung. Hier können die Schülerinnen und Schüler einfache Projekte mit dem Mikrokontroller Calliope umsetzen. Abschließend finden Sie ein Großprojekt zum Calli:bot.

Automaten programmieren und simulieren

Automaten spielen in vielen Lebensbereichen eine große Rolle. Daher wird ein tiefgreifendes Verständnis über die Funktionsweise und Programmierung von Automaten immer wichtiger. Mit den benutzerfreundlichen Online-Tools Flaci und Kara stehen den Schülerinnen und Schülern zwei Möglichkeiten zur Erstellung und Simulation von Automaten zur Verfügung.

Mit Informatik 9/10 werden Ihre Schülerinnen und Schüler:

- einen einfachen und spannenden Zugang in die Automatentheorie erhalten
- endliche Automaten theoretisch verstehen und praktisch anwenden
- Automaten zu programmieren geschult
- visuell lernen, wie Automaten erstellt und simuliert werden

Entdecken Sie unsere Lehr- und Lernwelten für den Informatikunterricht in den Jahrgangsstufen 5 und 6:

Informatik – Nordrhein-Westfalen

Informatik – Nordrhein-Westfalen - Differenzierende Ausgabe

Das macht unsere Reihen aus:

- geeignet für alle Schularten
- anschauliche Aufbereitung der Inhalte
- Verankerung der Inhalte in der Lebenswelt der Schülerinnen und Schüler
- konsequente Orientierung am Kernlehrplan
- Grundlagen der Algorithmik mithilfe der Programmierumgebung Scratch
- breites Aufgaben- und Differenzierungsangebot
- gezielte Vermittlung der Fachsprache
- integrierte digitale Materialien

interaktive h5p-Übungen, Erklärvideos und weitere **digitale Materialien** auch via QR- oder Mediencodes direkt in der Print-Ausgabe verfügbar

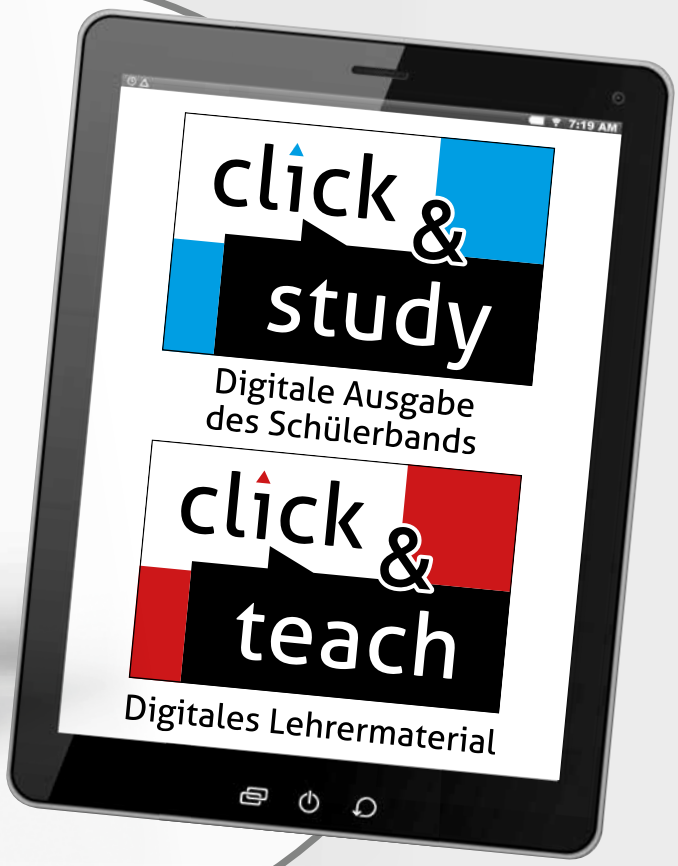
Informatik – Nordrhein-Westfalen

Sie haben

- informative Erarbeitungstexte
- Unterstützung der Darstellung durch visuelle Elemente
- inklusive weiterführender Materialien zur Vertiefung und Erweiterung der behandelten Inhalte
- umfangreiches Aufgabenangebot zur Auswahl
- handliches Buchformat
- vielseitige Einführung in Programme zur Anwendung des Unterrichtsinhalts

Mehr Infos
www.ccbuchner.de/bn/38041

click & study als Print-Plus-Lizenz
ab 1,90 € pro Titel und Jahr
bei Einführung der Print-Ausgabe

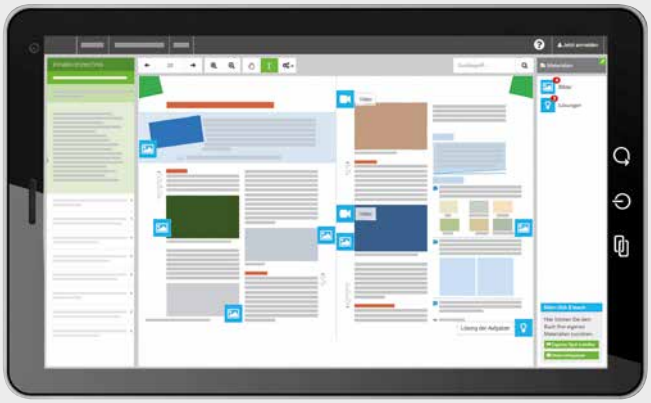


Ideal für den digitalen Materialaustausch

Die **digitale Ausgabe des Schülerbandes click & study** und das **digitale Lehrermaterial click & teach** bilden zusammen die ideale digitale Lernumgebung: vielfältig im Angebot und einfach in der Bedienung!

Mehr Infos finden Sie auf den Seiten 38 bis 41 und auf www.click-and-study.de und www.click-and-teach.de.

Demoversion
click & teach



die Wahl:

Band 5/6 inklusive digitalem Vorkurs Medienbildung

Informatik – Nordrhein-Westfalen
Differenzierende Ausgabe

- kompakte Texte in einfacher Sprache
- einprägsame Visualisierung der Inhalte
- Fokussierung auf die zentralen Inhalte
- kleinschrittige Erarbeitung der Inhalte
- machbares Aufgabenpensum
- großzügige Gestaltung im DIN-A4-Format
- große Schrift für eine bessere Lesbarkeit

Mehr Infos
www.ccbuchner.de/bn/38121

click & study

Digitale Ausgabe des Schülerbands

Mit der digitalen Ausgabe des Schülerbands click & study und dem digitalen Lehrermaterial click & teach wird die Unterrichtsgestaltung und Vorbereitung einfacher als je zuvor.

Einfach in der Navigation:

Im Mittelpunkt steht immer die digitale Ausgabe des Schülerbands, um die sich alle Zusatzmaterialien und Funktionen gruppieren. So finden sich alle Inhalte dort, wo sie benötigt werden.

Einfach in der Bedienung:

click & study und click & teach bieten eine Fülle an nützlichen Funktionen. Die Gestaltung und die Bedienelemente sind dennoch nicht überladen und bleiben selbsterklärend.

Einfach im Zugriff:

Mit einem Internetbrowser können Sie mit jedem Endgerät auf click & study und click & teach zugreifen. Alternativ nutzen Sie die kostenfreie App – so können Sie auch offline arbeiten. click & study kann zudem via www.bildungslogin.de verwendet werden.

Einfach für alle:

click & study und click & teach können miteinander verknüpft werden. So funktioniert der Unterricht bei Bedarf komplett digital – ideal für Tablet-Klassen und den digitalen Materialaustausch zwischen Lehrenden und Lernenden.

Weitere Informationen, kostenfreie Demoversionen und Erklärvideos finden Sie auf www.click-and-study.de und www.click-and-teach.de

click & teach

Digitales Lehrermaterial

Das und vieles mehr bieten click & study und click & teach:

Digitale Arbeitsseiten

Durch das Einfügen digitaler Arbeitsseiten besteht die Möglichkeit, auf einer zusätzlichen leeren Seite eigene Texte, Bilder, Links und Freihandzeichnungen zu hinterlegen.

Umfangreiches Lehrermaterial (nur in click & teach)

click & teach bietet umfangreiches digitales Zusatzmaterial wie zum Beispiel Lösungen, didaktische Hinweise, weitere digitale Lernanwendungen, Animationen, Arbeitsblätter, Kopiervorlagen, Tafelbilder und vieles mehr.

Lerngruppenfunktionen

Als Lehrkraft haben Sie in click & teach die Möglichkeit, Materialien in click & study freizuschalten. Im Aufgabenpool und im Forum können Lernende Aufgaben digital empfangen, wieder abgeben und sich austauschen.

Lizenzmodelle für jeden Bedarf

Egal ob nur für Sie, das Kollegium oder die ganze Schule – wir haben für jeden Bedarf ein passendes Angebot. Bestellen können Sie ausschließlich auf www.ccbuchner.de.

Lizenzmodelle click & teach

In click & teach sind immer die vollständige digitale Ausgabe des C.C.Buchner-Lehrwerks und umfangreiches Lehrermaterial enthalten. Die Laufzeit jeder click & teach-Lizenz gilt, solange das C.C.Buchner-Lehrwerk als gedrucktes Schulbuch lieferbar ist, in der Regel sind das mehrere Jahre. Inhaltlich sind alle Lizenzformen identisch.

click & teach	Einzellizenz	Einzellizenz Box	Einzellizenz flex	Kollegiums-lizenz
Lizenz-anzahl	1	1	1	beliebig viele Lizenzen für Ihr Fachkollegium (inkl. Referendare)
Weitergabe	nicht übertragbar	nicht übertragbar	übertragbar*	für das komplette Fachkollegium (inkl. Referendare)
Zugang	digitaler Freischaltcode per E-Mail	Box inkl. Karte mit Freischaltcode per Post	direkte Freischaltung im Schulkonto	direkte Freischaltung im Schulkonto
Verfüg-barkeit	im persönlichen Nutzerkonto	im persönlichen Nutzerkonto	im verknüpften Schulkonto	im verknüpften Schulkonto

*Die Einzellizenz flex kann beliebig oft an eine andere Person übertragen werden.

Schulkonto

Auf www.ccbuchner.de können sich Lehrkräfte (auch jene im Referendariat) mit ihrem Schulkonto verknüpfen und folgende Funktionen nutzen:

- **click & teach-Lizenzen erwerben und nachkaufen**
  In wenigen Schritten können über die Auswahl des Fachs und des Bundeslands die Kollegiumslizenz sowie die Einzellizenzen flex per Rechnung an die hinterlegte Schule erworben werden. So kann click & teach direkt genutzt werden – ohne Wartezeit!
- **click & teach-Lizenzen verwalten und übertragen**
  Daneben kann die Zuordnung der Lizenzen zu Mitgliedern des Fachkollegiums eingesehen und verwaltet werden. Fachfremden Lehrkräften kann ebenfalls manuell eine Lizenz zugewiesen werden. Wurde eine Einzellizenz flex erworben, erfolgt im Schulkonto die Zuordnung bzw. die Übertragung.
- **Zugriffsrechte verwalten**
  Im Schulkonto können für alle verknüpften Kolleginnen und Kollegen die Rechte (*Lizenzen kaufen, Lizenzen verwalten, Zugriffsrechte bearbeiten, Schuldaten bearbeiten und Schulkollegium verwalten*) individuell vergeben werden.

Lizenzmodelle click & study

Auch in click & study ist immer die vollständige digitale Ausgabe des C.C.Buchner-Lehrwerks enthalten. Die Schülerinnen und Schüler erhalten Zugang zur digitalen Ausgabe über einen Freischaltcode, der per E-Mail an sie verschickt wird. Verfügbar ist click & study dann im persönlichen Nutzerkonto der Schülerinnen und Schüler. Die Lizenzen sind nicht übertragbar.

click & study	Einzellizenz	Einzellizenz Print Plus
Preis	Normalpreis	Wenn das gedruckte Schulbuch eingeführt ist, ist pro Buch eine Jahreslizenz ab 1,90 € erhältlich.
Laufzeit	12 + 1 Monat ab Freischaltung	12 + 1 Monat ab Freischaltung
Lizenz-anzahl	1	1 pro eingeführtem Schulbuch

Stand: 01.01.2024

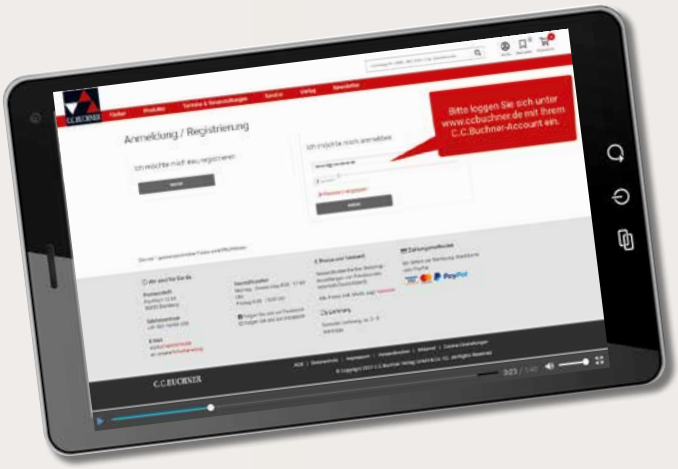
Sie haben Fragen?

Unsere Kolleginnen und Kollegen in der Digital-Beratung helfen Ihnen gern.

E-Mail: click-and-teach@ccbuchner.de | click-and-study@ccbuchner.de
Telefon: +49 951 16098333 | Mo, Mi, Fr: 10:00 – 11:30 Uhr | Di, Do: 14:00 – 15:30 Uhr

Weitere Informationen:
www.click-and-study.de
www.click-and-teach.de
www.ccbuchner.de/schulkonto

Erklärvideos Schulkonto



Unsere WebSeminare für Nordrhein-Westfalen

Wir unterstützen und begleiten Sie beim Umsetzen des aktuellen Kernlehrplans – und das nicht nur mit unseren neuen Lehrwerken. Wir möchten Ihnen Anregungen bieten, Materialien vorstellen und Gelegenheit zum Gedankenaustausch geben.

Deshalb bieten wir Ihnen WebSeminare an, für die Sie auch eine Teilnahmebestätigung erhalten.
Natürlich finden Sie uns ebenfalls auf überregionalen Messen und Kongressen.

Wir freuen uns auf spannende Veranstaltungen, auf gute Gespräche und vor allem auf Sie!

Detaillierte Informationen und Termine finden Sie auf www.ccbuchner.de/veranstaltungen.

Nichts mehr verpassen: Unser Newsletter mit allen aktuellen Terminen

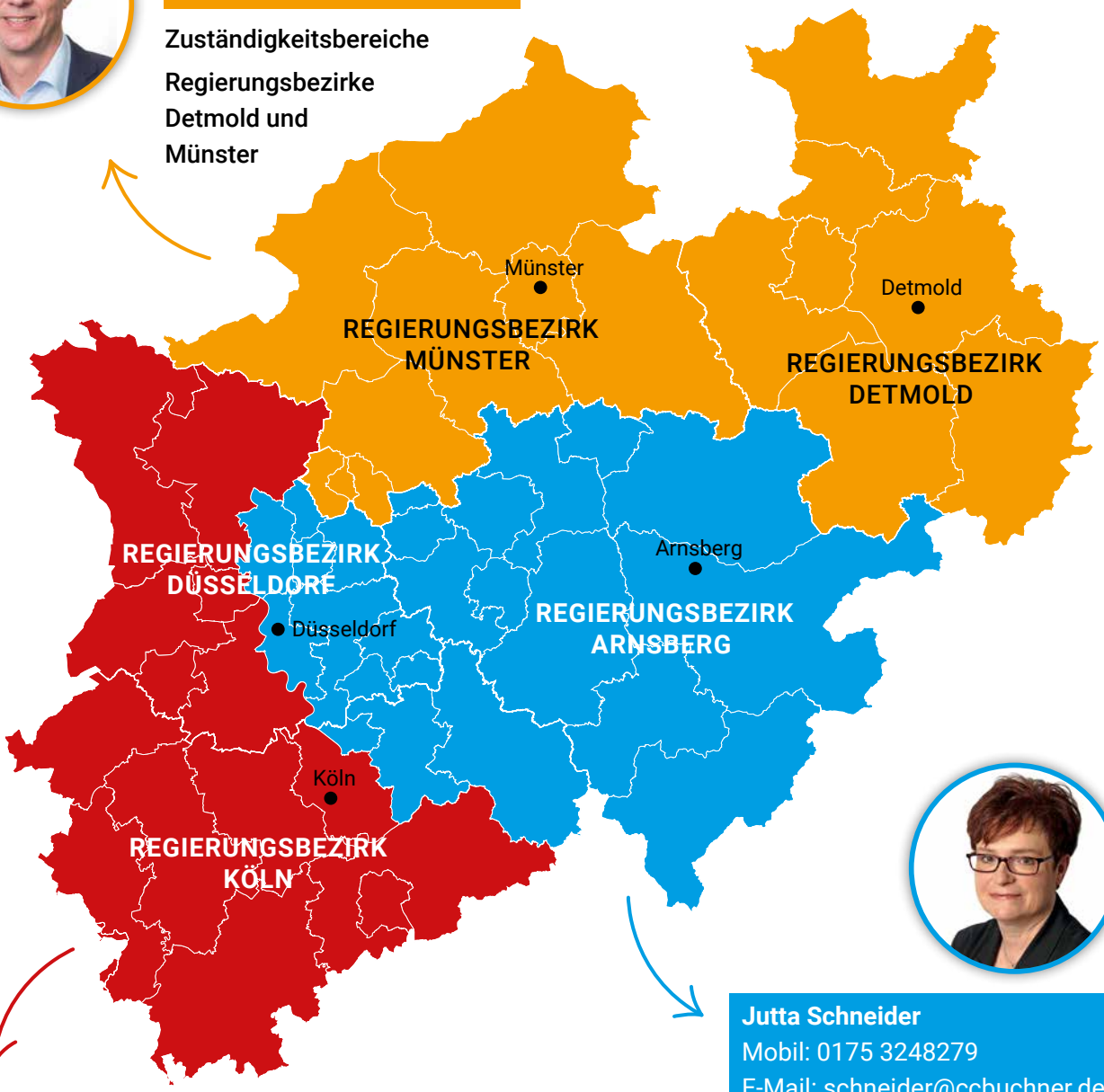
Abonnieren Sie jetzt unseren Veranstaltungsnewsletter!
Damit sind Sie fächerübergreifend immer über die aktuellen Termine von C.C.Buchner informiert und können sich Ihren Platz sichern.

Ihr Schulberatungsteam in Nordrhein-Westfalen

Jörn Thielke
Mobil: 0160 1728354
E-Mail: thielke@ccbuchner.de

Zuständigkeitsbereiche

Regierungsbezirke Detmold und Münster



Jutta Schneider
Mobil: 0175 3248279
E-Mail: schneider@ccbuchner.de

Zuständigkeitsbereiche

Regierungsbezirk Köln: Kreise Leverkusen, Oberbergischer Kreis, Rheinisch Bergischer Kreis

Regierungsbezirk Düsseldorf: Kreise Duisburg, Düsseldorf, Essen, Mettmann, Mülheim, Oberhausen, Remscheid, Solingen, Wuppertal

Regierungsbezirk Arnsberg

Monika Labmeier
Mobil: 0171 6357092
E-Mail: labmeier@ccbuchner.de

Zuständigkeitsbereiche

Regierungsbezirk Köln:
Kreise Aachen, Bonn, Düren, Euskirchen, Heinsberg, Köln, Rhein-Erft, Rhein-Sieg

Regierungsbezirk Düsseldorf:
Kreise Kleve, Krefeld, Mönchengladbach, Rhein-Kreis Neuss, Viersen, Wesel

Sie wünschen persönliche Beratung?
Unser Schulberatungsteam für Nordrhein-Westfalen ist für Sie da – vor Ort, telefonisch und online:

Monika Labmeier
Mobil: 0171 6357092
E-Mail: labmeier@ccbuchner.de

Jutta Schneider
Mobil: 0175 3248279
E-Mail: schneider@ccbuchner.de

Jörn Thielke
Mobil: 0160 1728354
E-Mail: thielke@ccbuchner.de

Sie benötigen weitere Exemplare dieser Leseprobe* für Ihre Fachkonferenz?

1. Geben Sie auf **www.ccbuchner.de** die Bestellnummer **L38043** in die Suchleiste ein.
2. Legen Sie die kostenfreie Leseprobe (1 Exemplar pro Person) und ggf. weitere Produkte in Ihren **Warenkorb**.
3. Folgen Sie den weiteren Anweisungen, um den Bestellvorgang abzuschließen.

L38043

+ **Oder direkt über:**

*Nur solange der Vorrat reicht.

C.C.BUCHNER L38043