„Nicht für Fremde bestimmt!" – Daten sicher handhaben

Einfache Verschlüsselungsverfahren kennen

Kryptografie

Das griechische Wort „kryptos" bedeutet verborgen, geheim; „Grafie" steht für Schreibung, Schreibweise. Die Kryptografie beschäftigt sich also mit der Frage, wie man Informationen so codieren kann (vgl. S. 10–13), dass nur Eingeweihte sie lesen können.
Im Zusammenhang mit digitalisierten Daten umfasst Kryptografie folgende Funktionen:

- **Vertraulichkeit/Zugriffsschutz:** Daten oder Nachrichten dürfen nur von berechtigten Personen gelesen werden. ☐
- **Änderungsschutz:** Daten müssen nachprüfbar vollständig und unverändert sein. ☐
- **Authentizität/Fälschungsschutz:** Der Absender einer Nachricht muss zweifelsfrei identifizierbar sein. ☐

Kryptoanalyse ist im Gegenzug die Wissenschaft vom „Knacken" verschlüsselter Botschaften.

1 Prüfe, welche Funktionen der Kryptografie die im Comic oben getroffenen Maßnahmen erfüllen.
Trage im Info-Kasten ein: *V* = Verschlüsselung, *S* = Siegel.

2 Angeblich hat Julius Cäsar eine Methode zur Verschlüsselung von Nachrichten erfunden.

a) Die folgende Tabelle ist der „Schlüssel" zum sogenannten Cäsar-Code, mit dem man diesen anwenden kann. Vervollständige sie.
Tipp: Die Abbildung rechts hilft dir.

Klarschrift

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

Geheimschrift

b) Erschließe die Nachricht im Comic oben mit diesem Schlüssel.

3 Man kann eine Nachricht auch verschlüsseln, indem man Zeichen, hier: die Buchstaben des Alphabets, durch andere Zeichen ersetzt. Das können Bilder sein, aber auch Buchstaben, z. B. so:

Klarschrift

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

Geheimschrift

a) Beschreibe den Unterschied zwischen dieser Methode und dem „Cäsarcode" bei Aufgabe 2.

b) Wähle eine Lernpartnerin/einen Lernpartner: Überlegt, welche der beiden Arten der Verschlüsselung sicherer ist, und begründet eure Einschätzung.

Verfahren für Zugriffsrechte auf Daten und Geräte kennen und anwenden

Ein Passwort anlegen

Mit einem Passwort stellt man sicher, dass niemand Fremdes z. B. einen Computer, ein Smartphone, eine bestimmte Datei oder einen Internetzugang benutzen kann. Es funktioniert ähnlich wie ein **Schlüssel** in der realen Welt. Nur der Besitzer oder jemand, dem er das Passwort weitergegeben hat, kann auf Daten oder Geräte zugreifen.

Wie sieht ein gutes Passwort aus?
Ein gutes Passwort sollte **mindestens acht Zeichen** lang sein, **13 Zeichen** sind **sicherer.** Ein Passwort sollte niemals nur aus einem Wort (oder Namen) bestehen. Auch Jahreszahlen sollten nicht verwendet werden.
Geeignet ist eine Kombination aus Ziffern, Buchstaben (groß- und kleingeschrieben) und Sonderzeichen, z. B. **HgfN8t9@!1#zW.**

Wie bleibt ein Passwort sicher?
Damit ein Passwort seine Funktion nicht verliert, muss es **geheim** bleiben. Aus diesem Grund sollte es nicht oder nur an einem sehr sicheren Ort aufgeschrieben werden. Niemals dort, wo es gebraucht wird!
Ein Passwort sollte auch **regelmäßig geändert** werden. Existiert es zu lange, ist das Risiko höher, dass es sich jemand unbemerkt angeeignet hat. Auch Passwörter, die mehrfach für unterschiedliche Anwendungen genutzt werden, sind gefährdet. Man sollte besser für **jeden Zweck ein anderes Passwort** wählen.

1 a) Passwort-Check: Kreuze jede Aussage an, die auf dein Passwort zutrifft.

Mein Passwort

- ☐ … ist ein Wort, das man in einem Wörterbuch finden kann.
- ☐ … ist kürzer als 6 Zeichen.
- ☐ … benutze ich für viele verschiedene Webseiten und Geräte.
- ☐ … habe ich aufgeschrieben und neben meinen Computer gehängt, damit ich es nicht vergesse.
- ☐ … nutze ich bereits seit mehreren Jahren, damit ich es nicht vergesse.
- ☐ … kennt auch mein bester Freund/meine beste Freundin.

b) Werte deine Antworten im Hinblick auf die Informationen im Kasten oben aus: Ist dein Passwort sicher? Falls nicht: Was musst du verändern?

2 Lege ein neues, sicheres Passwort an.
Denk dir dafür einen Satz aus, den du dir gut merken kannst, z. B. → Mein Passwort knackt ganz sicher niemand!
Verteile die Anfangsbuchstaben der Wörter und füge an beliebiger Stelle Zahlen und Sonderzeichen ein. Überlege, wie du die Zeichen so anordnest, dass du das Passwort mühelos behältst.

Satz: _____

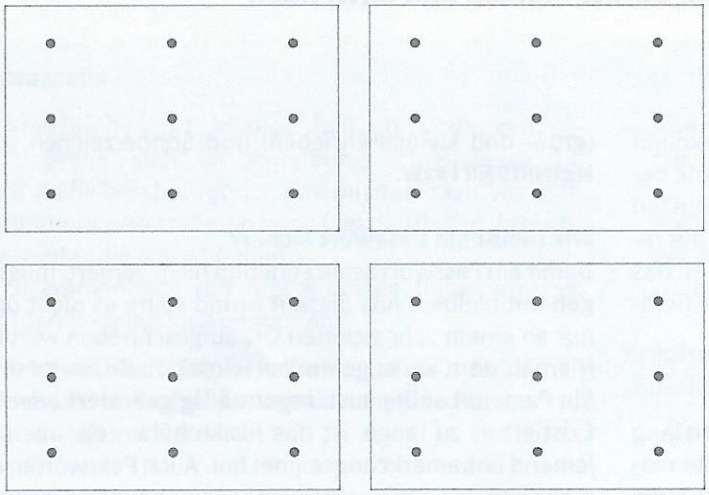
Passwort: | | | | | | | | | | | | | |

Individuelle Entsperrmuster

Manche Smartphones und Tablets bieten die Möglichkeit, das Gerät auch über die Eingabe eines **Musters** zu sperren. Dazu zeichnet man mit dem Finger auf dem Bildschirm ein vorher festgelegtes Muster nach. Vorteilhaft ist daran, dass man ein Gerät sehr schnell entsperren kann, wenn das Muster einfach ist.

3 Bestimmte Smartphones bieten neun Punkte als Bezugsrahmen für ein solches Muster an.

a) Es müssen jeweils mindestens drei Punkte verbunden werden. Zeichne vier unterschiedliche Muster ein.



b) Wähle einen Lernpartner/eine Lernpartnerin:
Person 1 fährt ein Muster auf dem Tisch nach. Person 2 beobachtet und versucht, das Muster nachzuzeichnen. Wechselt.

c) Wertet aus: Wie sicher ist dieser „Zugangsschlüssel"? _____

Biometrische Authentifikation

„Authentifikation" bedeutet, dass die **Identität eines Nutzers geprüft** wird, bevor er Zugang zu einem System bekommt. „Biometrie" bedeutet, dass z. B. **biologische Informationen** mathematisch verarbeitet, also mit Zahlen erfasst werden. Interessant sind hier Fingerabdruck, Auge (Iris-Erkennung), Stimme oder Gesicht, denn sie sind bei jedem Menschen einzigartig.

Verfügt ein Gerät über eine **Kamera** oder einen **Sensor,** kann es solche Merkmale scannen und im System hinterlegen (Beispiel: Face-ID). Vor jedem Zugriff werden sie dann abgeglichen.

4 Prüfe, ob dein Smartphone über Funktionen für eine biometrische Authentifizierung verfügt.
Richte eine Face-ID ein. Probiere dann aus, ob du das Handy mit einem Foto öffnen kannst.

PIN – Geheimzahl

Eine **P**ersönliche **I**dentifikations**n**ummer (PIN) ist eine vorher festgelegte Geheimzahl, die ihrem Anwender den Zugriff auf ein Smartphone oder einen Computer ermöglicht.

5 a) Frage in deiner Familie nach, nach welchen Kriterien jemand eine PIN festgelegt hat.

b) Gib eine begründete Empfehlung: Ist ein Geburtsdatum eine geeignete Grundlage für eine PIN?

6 Tauscht euch aus: Welche Erfahrungen habt ihr mit Zugriffssicherungen gemacht?
Ordnet die folgenden Zugangsarten der Skala zu.

PIN | Fingerabdruck | Passwort | Entsperrmuster

eher unsicher ⟷ sehr sicher

Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung (2FA) bedeutet, dass man **zwei voneinander unabhängige Möglichkeiten** miteinander **kombinieren** muss, um Zugang zu bekommen. Alltagsbeispiele sind z. B.:
- Geldautomat: EC-Karte + PIN
- Online-Banking: Anmeldenummer + TAN*
- Zugang zu einem Gebäude: Face-ID + PIN

* **T**rans**a**ktions**n**ummer

Es können auch bestimmte Gegenstände dafür bereitgestellt werden, wie eine EC-Karte (mit Chip), ein Generator für Nummern oder ein Schlüssel. Diese Gegenstände muss man dann aber stets verfügbar halten. Zunehmend werden diese Funktionen auch in Smartphone-Apps ausgelagert, weil man dieses immer bei sich führt und keine weiteren Geräte benötigt.

7 Erkläre deiner Familie den Begriff „Zwei-Faktor-Authentifizierung" und finde heraus, in welchen Zusammenhängen diese privat oder beruflich angewendet wird. Lass dir ggf. die benötigten Gegenstände dafür zeigen. Notiere mindestens zwei Beispiele.

8 Damit man sich mit dem Smartphone authentifizieren kann, muss eine wichtige Voraussetzung erfüllt sein. Überlege und erkläre, welche das ist.

Formulare mit „Captcha" authentifizieren

Bei Bestellungen oder Anträgen im Internet bekommt man abschließend oft eine Aufgabe, z. B., einen Code aus völlig verschobenen Zeichen zu lesen und einzugeben oder einen verfremdeten Gegenstand auf einem Foto zu erkennen. Diese **Aufgaben** sind so angelegt, dass sie **nur von einem Menschen ausgeführt** werden können. Man will damit ausschließen, dass Bots (Roboterprogramme) Schaden anrichten. Allerdings werden diese immer leistungsfähiger und können solche Muster „knacken"!

9 Berichtet in der Klasse, welche „Captcha"-Aufgaben ihr kennt und in welchen Zusammenhängen sie aufgetreten sind.

Datenmissbrauch: Risiken (er)kennen

Passwörter können – mit mehr oder weniger Aufwand – geknackt werden. Weil sie an persönliche Daten herankommen wollen oder z. B. an fremde Bankkonten, investieren Menschen ziemlich viel kriminelle Energie darauf. Diese Seite zeigt zwei Beispiele.

Brute-Force-Angriff

„Brute Force" bedeutet rohe Gewalt, gemeint ist jedoch eine **automatisierte Methode, Passwörter** durch **Ausprobieren von Kombinationen** zu knacken. Brute-Force-Angriffe probieren einfach alle potenziell möglichen Zeichenreihenfolgen aus. Schnelle Rechner können zwei Milliarden Zeichenkombinationen pro Sekunde und mehr durchlaufen lassen. Bei einem Passwort, das nur aus Groß- und Kleinbuchstaben besteht und eine Länge von fünf Zeichen hat (19.770.609.664 mögliche Kombinationen), könnte eine Software es in nur 9,89 Sekunden garantiert knacken. Umfasst ein Passwort neun Zeichen, müsste der Computer bereits 16,09 Tage lang rechnen. Um vor diesem Hintergrund die **Sicherheit** zu erhöhen, erzwingen viele Geräte (z. B. Smartphones) oder Programme eine Wartezeit, nachdem man dreimal das falsche Passwort eingegeben hat. Nach zehn falschen Eingabeversuchen wird das Gerät vom Anbieter meist vollkommen gesperrt.

1 a) Erkläre: Warum brauchen Computer bei einem längeren Passwort mehr Zeit, um es zu knacken?

b) Beurteile die im Text dargestellten Maßnahmen zur Erhöhung der Sicherheit: Was bewirken sie?

Phishing

Angreifer versuchen, Zugangsdaten für z. B. Online-Banking oder Bezahldienste zu erschleichen. Gefälschte E-Mails, angeblich von einer Bank oder einem Online-Shop, fordern den Empfänger auf, über einen Link auf eine Login-Seite zu gehen und dort Anmeldedaten einzugeben. Der Link führt zu einer gefälschten Seite. Gibt jemand dort seine Daten ein, erhält er eine Fehlermeldung. Die Betrüger nehmen die Daten aber trotzdem entgegen und melden sich damit selbst z. B. in einem Online-Shop an, um auf Rechnung des Kunden dort einzukaufen.

2 Ordne den Tipps zum Erkennen von Phishing-Versuchen die richtigen Beispiele zu: Trage die Buchstaben passend in die linke Spalte ein.

Daran erkennt man Phishing	Beispiele
1 ☐ Die Anrede ist in der Regel unpersönlich.	A „Bitte tragen Sie hier Ihr Passwort und Ihre PIN-Nummer ein."
2 ☐ Man wird aufgefordert, sofort zu reagieren.	B „Ich mache auf diesen dringenden Problem aufmerksam."
3 ☐ Die Mail enthält eine Drohung.	C „Lieber Kunde, liebe Kundin, ..."
4 ☐ Es wird nach vertraulichen Daten gefragt.	D „Bitte ändern Sie aus Sicherheitsgründen sofort Ihr Passwort."
5 ☐ Oft sind Phishing-Mails in schlechtem Deutsch verfasst.	E „Sollten Sie der Aufforderung nicht folgen, werden wir Ihr Konto sperren."

Sichere Übertragungswege für Daten einstellen und prüfen

1 Schaut euch den Cartoon an und klärt, warum man elektronische Kommunikation verschlüsseln sollte.

Verschlüsselungstechniken im WWW

Damit die Datenübermittlung in einem Netzwerk funktioniert, verwendet man sogenannte **Schichtenmodelle,** die die Aufgabenbereiche der Komponenten und Schnittstellen festlegen. Sie beinhalten Übertragungsprotokolle, die u. a. für Datensicherheit sorgen:

- Das **Übertragungsprotokoll SSL** (Secure Sockets Layer, Layer = Schicht) bzw. dessen Nachfolger **TLS** (Transport Layer Security) sichern z. B. Daten im **E-Mail-Verkehr** ab.
- Das **HTTP-Protokoll** legt fest, wie **Webseiten** beim Surfen von Servern angefordert und zum Browser des Anwenders übertragen und angezeigt werden (vgl. S. 36). Wenn bei einem Browser die Verbindung über SSL abgesichert ist, heißt diese **HTTPS**. Moderne Browser zeigen sichere Verbindungen zusätzlich durch ein Symbol an.

2 Sicherheitscheck für deine Internetnutzung:

a) Gib an: Welchen Browser nutzt du überwiegend?

_____

b) Gib eine Internetadresse deiner Wahl ein.
Siehst du das Zeichen für eine sichere Verbindung? ☐ ja ☐ nein

c) Notiere: Welchen E-Mail-Dienst nutzt du überwiegend? _____

d) Recherchiere, wie man bei deinem Dienst eine SSL-/TSL-Verschlüsselung einstellt, und richte sie ein.

e) Klicke in deiner Messenger-App auf „Einstellungen" → „Sicherheit" und mache dich mit den Optionen vertraut. Prüfe: Gibt es eine Verschlüsselung? Kann man die Zwei-Faktor-Authentifizierung einstellen? Optimiere deine Einstellungen so, dass sie das für dich größte Maß an Sicherheit und Komfort bieten.

3 Recherchiere, wie man mit deinem Betriebssystem Daten auf einem USB-Stick verschlüsseln kann. Prüfe auch, ob es dafür geeignete und kostenlose Software gibt.
Sichere deinen USB-Stick mit einem Passwort und einer Verschlüsselung.