UNTERRICHTSMODUL KOMMUNIKATIONS- UND DIGITALTECHNIK

VERSCHLÜSSELUNG

ARBEITSBLATT UND LEHRERINFORMATION

Fachinhalte: Kodierung und Dekodierung von Informationen

Herausgeber: Arbeitgeberverband Gesamtmetall / **Autor:** Sebastian Funk / **Gestaltung:** YAEZ Verlag GmbH / **Titel- und Headerbild:** HandmadePictures (Shutterstock.com)

VERSCHLÜSSELUNG

VORAUSSETZUNGEN

Das Unterrichtsmodul lässt sich im Technikunterricht der 7. und 8. Klasse in weiterführenden Schulen einsetzen. Die Schülerinnen und Schüler sind vertraut mit einfacher Mathematik und den Methoden der Recherche sowie der Verwendung von Suchmaschinen im Internet. Sie benötigen für die Bearbeitung teilweise einen Onlinezugang, z. B. per WLAN oder über den Computerraum der Schule. Dieses Unterrichtsmodul vermittelt verschiedene Verschlüsselungsmethoden sowie das Kodieren und Dekodieren von Informationen als Grundlage kommunikationstechnischer Systeme zur Signalübertragung. Für Lehrerinnen und Lehrer bietet es sich an, bereits selbst Erfahrungen mit der E-Mail-Verschlüsselung PGP gesammelt zu haben. Weiterführende Informationen bietet zum Beispiel das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Den Link zur Website des Datenschutzzentrums finden Sie hier: me-vermitteln.de/datenschutz-info.

HINWEISE ZUM STUNDENABLAUF

GESAMTZEIT: 90 MINUTEN

PHASE	INHALT	ZEIT
1. Motivation	Den Schülerinnen und Schülern wird eine mit dem Caesar-Algorithmus verschlüsselte Nachricht vorgelegt, die Sie zuvor erstellt haben. Schreiben Sie die erforderliche Kodierungszahl für die Buchstabenverschiebung unkommentiert separat sichtbar auf. Sammeln Sie nach kurzer Bedenkzeit die Ideen der Schülerinnen und Schüler, was die Nachricht bedeuten könnte. Verweisen Sie zur Lösung auf die erste Bonusaufgabe.	10 Min.
2. Aufgabenstellung und Diskussion	Verteilen Sie die Arbeitsblätter und lassen Sie die Schülerinnen und Schüler Aufgabe 1 und 2 bearbeiten. Geben Sie den Schülerinnen und Schülern Zeit, das Schema der Verschlüsselung herauszufinden. Bei Bedarf können Sie Hinweise geben. Beide Aufgaben halten einen Bonus für schneller lernende Schülerinnen und Schüler bereit. Gehen Sie bei der Diskussion nach Aufgabe 3 auf die von den Schülerinnen und Schülern entwickelten Verschlüsselungsmethoden ein. Sammeln Sie die besten Schlüssel der Klasse für die spätere Sicherung.	40 Min.
3. Recherche und Diskussion	Bei Aufgabe 4 empfiehlt sich die Nutzung einer Internetverbindung für breitere Recherchemöglichkeiten. Die Schülerinnen und Schüler tragen ihre Ergebnisse zum PGP-Schema vor. Diskutieren Sie anschließend die Vor- und Nachteile der PGP-Verschlüsselung im Vergleich zu symmetrischen Verschlüsselungsverfahren.	30 Min.
4. Sicherung und Hausaufgabe	Die Schülerinnen und Schüler notieren sich die bereits in Phase 2 gesammelten symmetrischen Schlüssel. Auch die Funktionsweise des PGP-Schemas sowie dessen Vor- und Nachteile werden notiert. Besprechen Sie nun die Hausaufgabe. Sollten Sie die Bonusaufgabe anbieten, geben Sie vor, wie Ihr öffentlicher Schlüssel an die Schülerinnen und Schüler übermittelt wird.	10 Min.

HAUSAUFGABE: DIE VERSCHLÜSSELTE E-MAIL

Die Schülerinnen und Schüler sollen herausfinden, wie sie für ihr E-Mail-Programm eine PGP-Verschlüsselung verwenden können und eine Anleitung dazu notieren. Für eine Bonusaufgabe können Sie Ihren öffentlichen Schlüssel per E-Mail an Ihre Schülerinnen und Schüler senden, damit sie Ihnen eine mit PGP verschlüsselte E-Mail schicken können.

BINNENDIFFERENZIERUNG

- ▶ Die Basisaufgabe ist von allen Schülerinnen und Schülern zu lösen.
- ▶▶ Die Bonusaufgabe ist optional, sie dient als Reserve oder Ergänzung für leistungsstärkere Lernende.

VERSCHLÜSSELUNG

E-Mails sind in der heutigen Wirtschaftswelt die Methode, um wichtige Betriebsinformationen weltweit auszutauschen. Dabei ist die Geheimhaltung der Informationen absolut wichtig für den Erfolg des Unternehmens. Die folgenden Aufgaben sollen dir einen Einblick in die Funktionsweisen verschiedener Verschlüsselungstechniken geben.

AUFGABEN

▶ Basisaufgabe ▶▶ Bonusaufgabe

1. SYMMETRISCHE VERSCHLÜSSELUNG: DER KLEINE CAESAR

- ▶ Untersuche die nebenstehende Tabelle und finde heraus, nach welchem Schema das Kodieren der Geheimschrift funktioniert.
- ▶ Schreibe einen Satz auf und kodiere ihn mit dieser Caesar-Verschlüsselung.
- ▶ Tausche deine Nachricht mit einem Mitschüler. Übersetze die verschlüsselte Nachricht, indem du die Verschiebung rückwärts anwendest.
- ▶▶ Entschlüssle die Nachricht deines Lehrers vom Beginn der Stunde.

MATERIAL KLEINER CAESAR

KLAR	A	B	C	D	E	F	G	H	I	J	K	L	M
GEHEIM	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**

KLAR	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GEHEIM	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**

2. VERSCHLÜSSELUNGEN MIT KODIERUNGSSCHLÜSSEL

- ▶ Dekodiere das Wort „XWTWTG“, es wurde mit dem Schlüssel „GEHIMSCRFT_E“ verschlüsselt.
- ▶ Finde nun heraus, wie der Schlüssel „GEHIMSCRFT_E“ entstanden ist. Notiere deine Erkenntnisse schrittweise.
- ▶▶ Wähle nun selbst ein Schlüsselwort und notiere eine Kodierungstabelle mit deinem Schlüssel.

MATERIAL KODIERUNGSSCHLÜSSEL

KLAR	A	B	C	D	E	F	G	H	I	J	K	L	M
GEHEIM	**W**	**X**	**Y**	**Z**	**G**	**E**	**H**	**I**	**M**	**S**	**C**	**R**	**F**

KLAR	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GEHEIM	**T**	**A**	**B**	**D**	**J**	**K**	**L**	**N**	**O**	**P**	**Q**	**U**	**V**

3. EIGENE VERSCHLÜSSELUNGS-TECHNIKEN

- Entwickelt in Gruppen von 3 Personen eine eigene Buchstabenverschlüsselung nach dem Vorbild aus Aufgabe 1 oder 2 und kodiert eine Nachricht mit dieser.
- Damit die Empfängergruppe der Botschaft eure Nachricht entschlüsseln kann, benötigt sie den Schlüssel, sowie die Kenntnis über die Verschlüsselungsmethode. Notiert eure Verschlüsselungsmethode auf das freie Feld dieses Arbeitsblattes und übermittelt den Schlüssel an die Empfänger eurer Botschaft.
- Stellt gemeinsam als Gruppe eure Verschlüsselungsmethode der Klasse vor. Diskutiert dabei, welcher Schlüssel die zum Kodieren einfachste Methode ist und welcher Schlüssel die einfachste Methode zur Dekodierung ist.

MATERIAL MEIN KODIERUNGSSCHLÜSSEL

NOTIERE HIER DEINEN SCHLÜSSEL ZUR KODIERUNG UND DEKODIERUNG:

KLAR	A	B	C	D	E	F	G	H	I	J	K	L	M
GEHEIM													

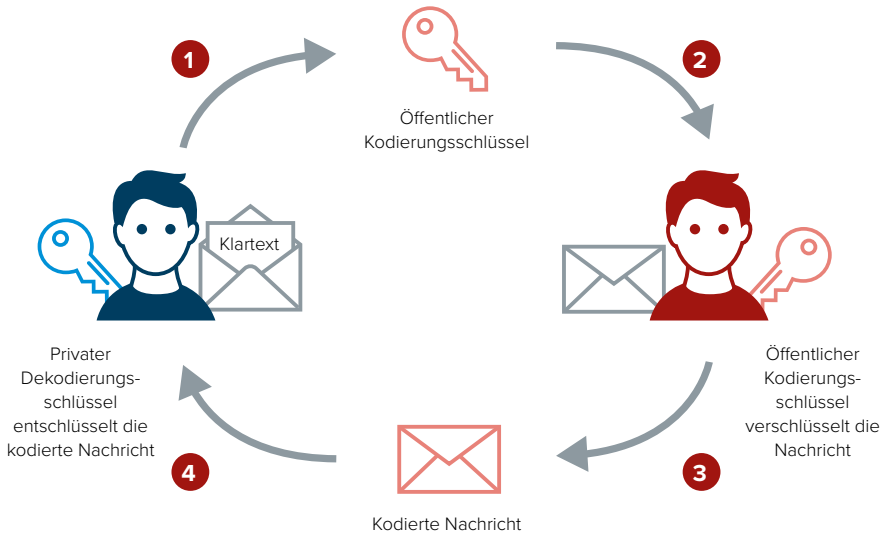
KLAR	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GEHEIM													

4. PGP-VERSCHLÜSSELUNG UND DEKODIERUNG

Eine sehr sichere Methode der E-Mailverschlüsselung ist die PGP-Verschlüsselung. PGP steht für pretty good privacy, ziemlich gute Privatsphäre, und ist ein asymmetrisches Verschlüsselungsschema. Im Gegensatz zur symmetrischen Verschlüsselung gibt es zwei Schlüssel. Der erste verschlüsselt die Nachricht, der zweite entschlüsselt die Nachricht. Im Schaubild siehst du schematisch, wie die PGP-Verschlüsselung funktioniert.

- Recherchiere, was ein öffentlicher und ein privater Schlüssel bei der PGP-Verschlüsselung sind.
- Beschreibe gemeinsam mit deiner Gruppe den Verschlüsselungsverlauf der E-Mail anhand des Schaubildes und notiere eure Ergebnisse.

MATERIAL DIE PGP-VERSCHLÜSSELUNG



- Welche Vor- und Nachteile bietet die PGP-Verschlüsselung unter Berücksichtigung der Sicherheit? Sammle zuerst Argumente und diskutiere diese dann in deiner Gruppe.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

1. SYMMETRISCHE VERSCHLÜSSELUNG: DER KLEINE CAESAR

Der kleine Caesar ist eine der leichtesten Verschlüsselungsmethoden. Der gleiche Schlüssel ver- und entschlüsselt eine Nachricht. Dazu wird diese mit jeweils einer freien Zeile auf Kästchenpapier notiert. Pro Kästchen ein Buchstabe. In die freie Zeile werden mit einem andersfarbigen Stift die kodierten Buchstaben eingetragen. Jeder Buchstabe der Nachricht wird um eine bestimmte Anzahl im Alphabet nach rechts verschoben. Im vorliegenden Beispiel um zwei Buchstaben. So wird aus dem A im Klartext ein C im Geheimtext.

Beim Empfänger der Nachricht ist es ratsam, nicht den jeweiligen Sitznachbarn zu wählen. Besprechen Sie im Vorfeld klare Verhaltensregeln bzgl. der Lautstärke in der Klasse, wenn die Schülerinnen und Schüler ihre Nachrichten an andere übermitteln.

Schülerinnen und Schüler, die die Aufgaben bereits erledigt haben, können die Bonusaufgabe lösen.

2. VERSCHLÜSSELUNG MIT KODIERUNGSSCHLÜSSEL

Ein Kodierungsschlüssel kann auch ein Wort sein. Im Beispiel auf dem Schülerarbeitsblatt ist es das Wort „Geheimschrift“. Geben Sie Ihren Schülerinnen und Schülern auch hier zunächst Zeit, die Funktionsweise der Verschlüsselungsmethode herauszufinden. Erklären Sie bei Bedarf oder nach Ablauf der Zeit selbst, wie das Kodierungsverfahren funktioniert.

Das Schlüsselwort wird unter die Klarbuchstaben des Alphabets geschrieben. Bei doppelt auftretenden Buchstaben wird jeweils der zweite gestrichen. So wird aus „Geheimschrift“ der Schlüssel „GEHIMSCRFT“. Bei welchem Klarbuchstaben das Schlüsselwort anfängt, bestimmt ein Schlüsselbuchstabe, im Beispiel das „E“. Anschließend schreibt man die restlichen Geheimbuchstaben in alphabetischer Reihenfolge nach dem Schlüsselwort auf, wobei man die Buchstaben, die bereits im Schlüsselwort enthalten sind, auslässt. Der geheime Schlüssel lautet nun „GEHIMSCRFT_E“.

Das verschlüsselte Wort lautet im Klartext „Banane“.
Bonusaufgabe: Achten Sie darauf, dass Buchstaben nicht doppelt in der Geheimzeile der Kodierungstabelle auftauchen dürfen.

Der von den Schülerinnen und Schülern erstellte Schlüssel kann auch Grundlage einer vertiefenden Aufgabe sein, bei der eine Schülergruppe versucht, einen Schlüssel anhand eines verschlüsselten Satzes herauszufinden. Hilfestellungen können gegeben werden, indem für einzelne verschlüsselte Buchstaben die Klarbuchstaben angegeben werden.

3. EIGENE VERSCHLÜSSELUNGSTECHNIKEN

Bei den von den Schülerinnen und Schülern entwickelten Schlüsseln kann es durch sehr komplizierte Abläufe in der Kodierung zu Zeitproblemen kommen. Besprechen Sie daher im Vorfeld, dass die Schülerinnen und Schüler nur ein begrenztes Zeitfenster für die Aufgabe haben.

Die unterschiedlichen Kodierungsschlüssel können Sie zur Sicherung auch per Smartphone oder Kamera fotografieren.

Es besteht die Möglichkeit, dass eine Schülerin oder ein Schüler eine verschlüsselte Nachricht an zwei Empfänger senden kann. So entsteht kein Frust, falls die Schüleranzahl nicht gerade ist.

Im Anschluss an die Diskussion lassen Sie über die besten Schlüssel abstimmen und notieren diese für die spätere Sicherung.

4. PGP-VERSCHLÜSSELUNG UND DEKODIERUNG

Unter Eingabe des Suchbegriffs „PGP-Verschlüsselung“ finden die Schülerinnen und Schüler zahlreiche Erklärungen, Videos und Grafiken zu diesem Thema. Empfehlenswert ist der Link auf me-vermitteln.de/verschluesseln-info, hier finden Sie die Website zum Selbstdatenschutz.

Eine Musterlösung kann sein: Der blaue Empfänger lässt seinen öffentlichen Schlüssel dem roten Sender zukommen. Der Sender verschlüsselt seine Nachricht mit dem öffentlichen Schlüssel des Empfängers und leitet die kodierte Nachricht an den Empfänger weiter. Die Nachricht wird dann vom Empfänger mit seinem privaten Schlüssel entschlüsselt.

Vorteil: Dank der asymmetrischen Schlüssel ist dies (je nach Stärke des Schlüssels) das sicherste Verschlüsselungsverfahren.

Nachteil: Der Empfänger muss seinen öffentlichen Schlüssel sicher zum Sender bringen. An dieser Stelle können Sie auch das Thema vertrauensvolle Signatur besprechen.