WHAT ABOUT ME

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

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**

Als Kopiervorlage freigegeben © Gesamtmetall 2017

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													

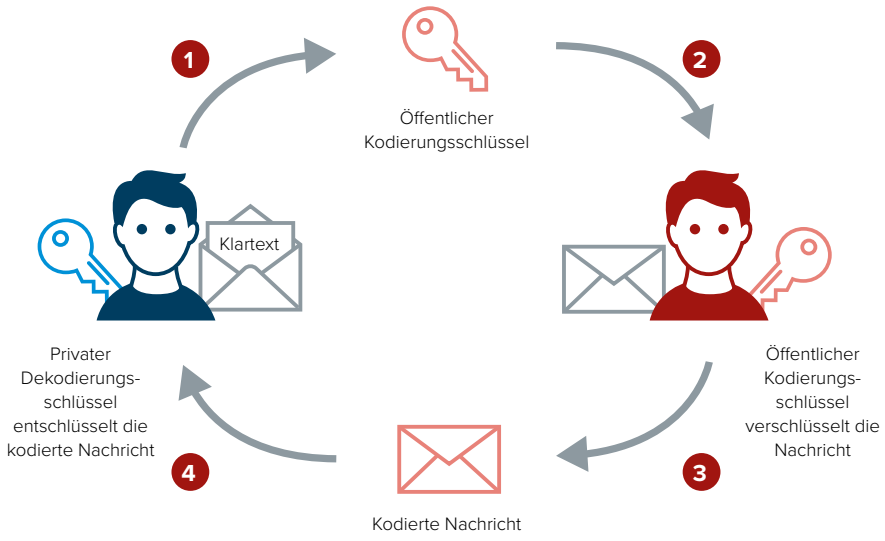
KLAR	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
GEHEIM													

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.

Als Kopiervorlage freigegeben © Gesamtmetall 2017