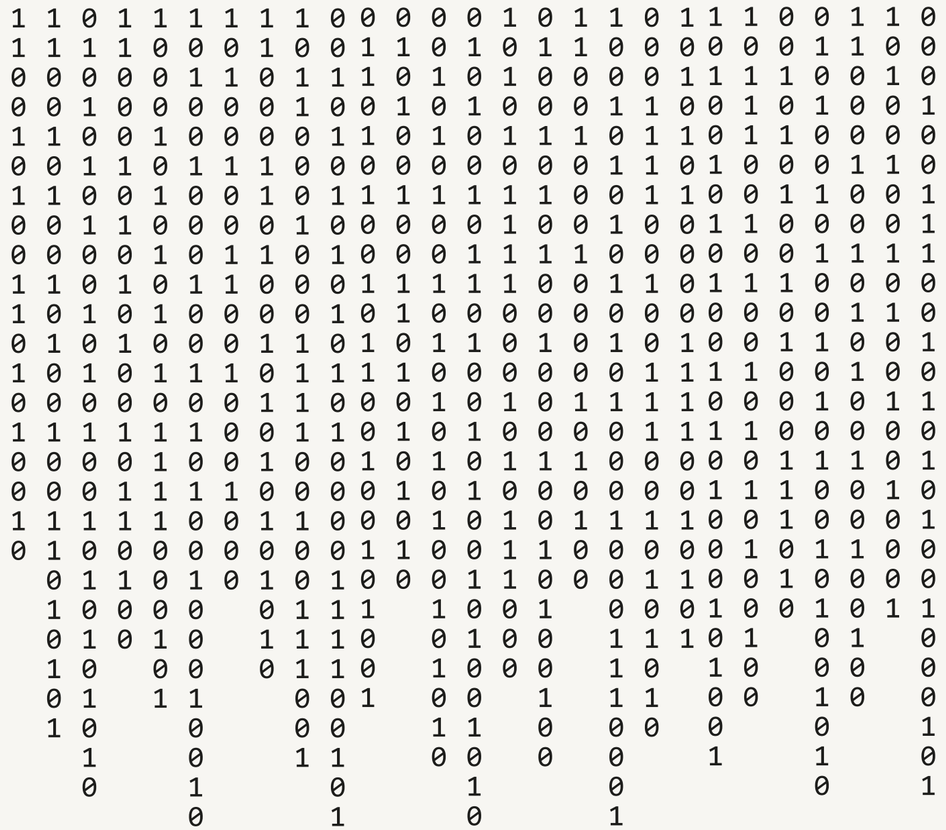


SICHERE KOMMUNIKATION

TAJA ZUCHTMANN

HILF 01.10.2024

ABLAUF

01 **Rahmenplan**
inhaltliche Orientierung

02 **Vorstellung**
Das bin ich.

03 **methodische Beispiele I**
aus dem eigenen Unterricht

04 **Aktivität**
digitale Spurensuche

05 **methodische Beispiele II**
aus dem eigenen Unterricht

06 **Inspirationen**
Empfehlungen und Links

RAHMENPLAN

Klasse 7

Sicher kommunizieren [MD] [BO] [DRF] [PG] **ca. 8 Unterrichtsstunden**

Die Gewährleistung der Vertraulichkeit ist eine Notwendigkeit für die Kommunikation im Internet und für die Sicherung der Privatsphäre.

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
Verschlüsselung verstehen	Verschlüsselung ist eine Codierung, bei der die Decodierung für Außenstehende nicht möglich sein soll.
• klassische Verfahren der symmetrischen Verschlüsselung anschaulich erläutern	Die Schülerinnen und Schüler beschreiben klassische Verfahren unter Verwendung der Begriffe Klartext- und Geheimtextalphabet, Klartext und Geheimtext, Schlüssel, Verschlüsseln und Entschlüsseln. Sie erkennen, dass durch Verschlüsselung eine vertrauliche Kommunikation ermöglicht wird.
• kurze Nachrichten verschlüsselt austauschen	Die Schülerinnen und Schüler argumentieren zur Sicherheit der Verfahren.
Vertraulichkeit herstellen • Möglichkeiten der Verschlüsselung in Standardprogrammen nutzen • verschlüsselte Daten als E-Mail-Anhang senden	
• Beispiele für verschlüsselte und unverschlüsselte Kommunikation nennen und eigene Kommunikation bewerten	Die Schülerinnen und Schüler kennen Indikatoren für die Verwendung verschlüsselter Kommunikationsprotokolle (z. B. gesichertes WLAN, https) bzw. informieren sich in geeigneten Quellen über die Sicherheitsmerkmale einer Kommunikation.
• Merkmale sicherer Kennwörter begründen und sichere Kennwörter verwenden	Bei der Wahl sicherer Kennwörter beachten die Schülerinnen und Schüler sowohl technische als auch psychologische Aspekte.
	Vorschlag zur inhaltlichen Vertiefung: Nutzung eigenständiger Programme für die Verschlüsselung und Komprimierung

RAHMENPLAN

Klasse 9

regionale Klasse 10

Prinzipien der Datenübertragung verstehen [MD] [BO] [DRF] **ca. 10 Unterrichtsstunden**

Die Schülerinnen und Schüler erweitern ihre Vorstellungen von Struktur und Arbeitsweise des Internets, um Konsequenzen der Übermittlung von Daten und Metadaten einschätzen und Schlussfolgerungen ableiten zu können.

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
grundlegende Prinzipien der Datenübertragung im Internet beschreiben • Prinzip der Adressierung • Prinzip der Namensauflösung • Prinzip der Zerlegung in Datenpakete • Prinzip der Protokolle • Prinzip des Routings • Prinzip der asymmetrischen Verschlüsselung	Die Prinzipien sind anschaulich und enaktiv-haptisch zu vermitteln. Die asymmetrische Verschlüsselung wird zur Sicherung der Vertraulichkeit, Authentizität und Integrität eingesetzt.

Digitalisierung in meiner Umgebung untersuchen **ca. 20 Unterrichtsstunden**
[MD] [BO] [BNE] [DRF] [PG]

Die Schülerinnen und Schüler untersuchen anhand eines geeigneten Kontexts Auswirkungen der Digitalisierung in ihrem unmittelbaren persönlichen Umfeld. Sie betrachten in diesem Zusammenhang auf Basis der zugrundeliegenden informatischen Konzepte Fragen der Sicherheit sowie soziale, rechtliche, ethische, ökologische und ökonomische Aspekte.

ca. 12 Unterrichtsstunden

Verbindliche Ziele und Inhalte	Hinweise und Anregungen

Aspekte der Digitalisierung verstehen
 	
• Eignung binärer Signale für die maschinelle Verarbeitung begründen
  - Bits logisch verknüpfen
  - binäre Addition
• Prinzip der asymmetrischen Verschlüsselung hinsichtlich Integrität, Vertraulichkeit und Authentizität untersuchen
	Die Aspekte sollten anschaulich und enaktiv-haptisch thematisiert werden.
	
	Die Schülerinnen und Schüler erkennen, dass die Verwendung eines Paares aus privatem und öffentlichem Schlüssel den Nachteil der symmetrischen Verschlüsselung – den geheimen Austausch eines gemeinsamen Schlüssels über eine öffentliche Verbindung – aufhebt.

RAHMENPLAN

Klasse 11/12

Sichere Kommunikation [MD2] [MD4] [DRF] **ca. 9/14 Unterrichtsstunden**

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
Aspekte der Kryptologie • Kommunikation mithilfe von Sequenzdiagrammen interpretieren und darstellen • die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen • die Sicherheit kryptografischer Verfahren mithilfe des Prinzips von Kerckhoffs prüfen • das Prinzip der asymmetrischen Verschlüsselung erläutern • die Prinzipien digital zertifizierter und signierter Daten erläutern • die Grenzen der modernen Kryptografie anhand der Einwegfunktionen erläutern [MD6]	Die Behandlung des Themas erfolgt anschaulich und ohne umfangreiche mathematische Berechnungen. Dazu können mono- und polyalphabetische Verschlüsselungsverfahren analysiert werden. Das One-Time-Pad ist als einzig sicheres Verfahren zu thematisieren. Das Prinzip der Einwegfunktion ist anschaulich darzustellen. Die Sicherheit der modernen Kryptografie beruht auf der Annahme, dass keine effizienten Verfahren für die Umkehrung der Einwegfunktionen existieren. Die Sicherheit kann weiterhin anhand der Ineffizienz von Brute-Force-Verfahren gezeigt werden.
zusätzlich für den Leistungskurs • das Prinzip der Einwegfunktion anhand einer Hashfunktion erläutern • das Prinzip der hybriden Verschlüsselung beschreiben und dessen Nutzen begründen	

VORSTELLUNG

Taja Zuchtmann

Don-Bosco-Schule Rostock
Mathematik und Informatik

Hausarbeit im Rahmen des 2. Staatsexamens für das Lehramt an Gymnasien

Erweiterung der Fachkompetenz im Prozessbereich Kooperieren und Kommunizieren mithilfe der Methode Stationsbetreib im Gegenstandsbereich des Sicheren Kommunizierens im Fach Informatik in Jahrgangsstufe 7 des gymnasialen Zweiges einer Gesamtschule

Datum	24.01.2020
Schule	Don-Bosco-Schule Rostock
Fach	Informatik
Klasse	7c
Uhrzeit	8:00 - 8:45 Uhr
Raum	147
Stunde in der Einheit	4/5

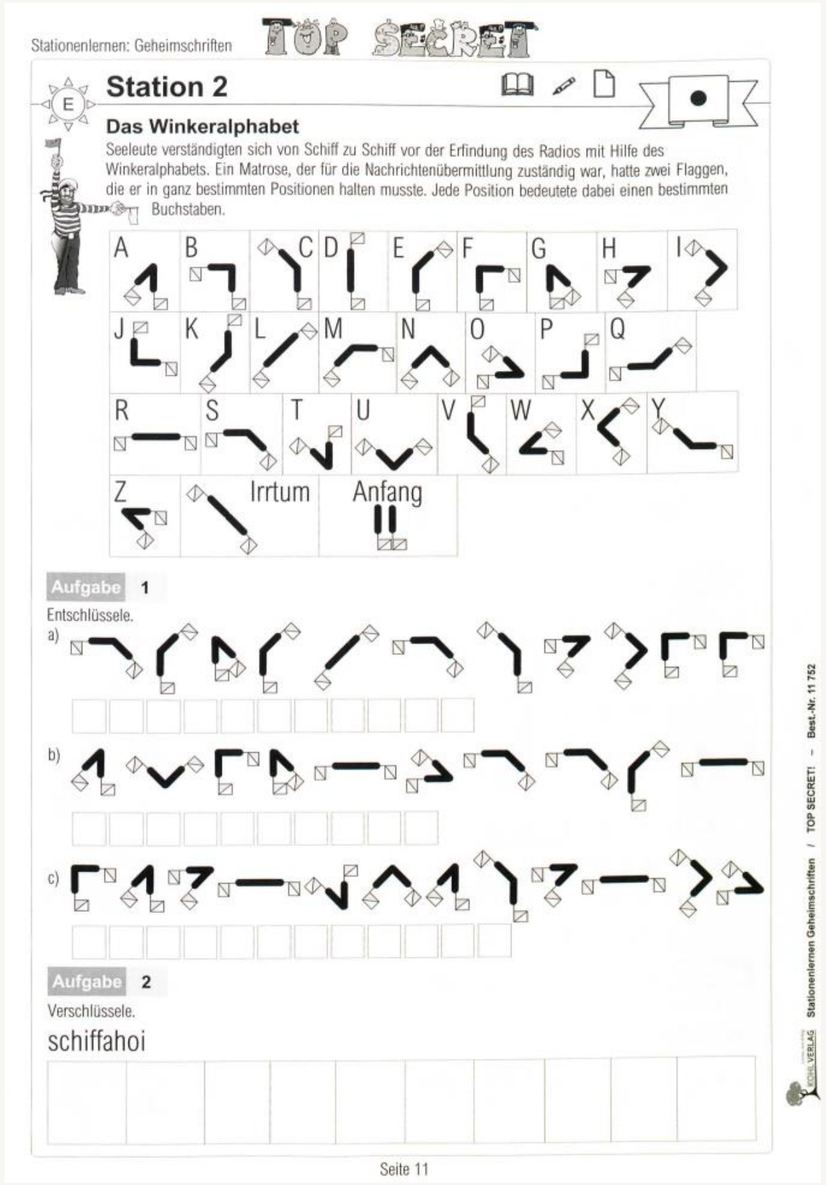
STATIONSLERNEN

Schmidt, H.-J. (2016, 2. Auflage): Stationenlernen Geheimschriften. Top Secret!. Köln: Kohl-Verlag.

INHALT

KOHL VERLAG Stationenlernen Geheimschriften / TOP SECRET! – Best.-Nr. 11 752

STATIONSLERNEN



Stationenlernen: Geheimschriften TOP SECRET

Station 2

Das Winkeralphabet

Seeleute verständigten sich von Schiff zu Schiff vor der Erfindung des Radios mit Hilfe des Winkeralphabets. Ein Matrose, der für die Nachrichtenübermittlung zuständig war, hatte zwei Flaggen, die er in ganz bestimmten Positionen halten musste. Jede Position bedeutete dabei einen bestimmten Buchstaben.

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 Irrtum Anfang

Aufgabe 1

Entschlüssele.

a)

b)

c)

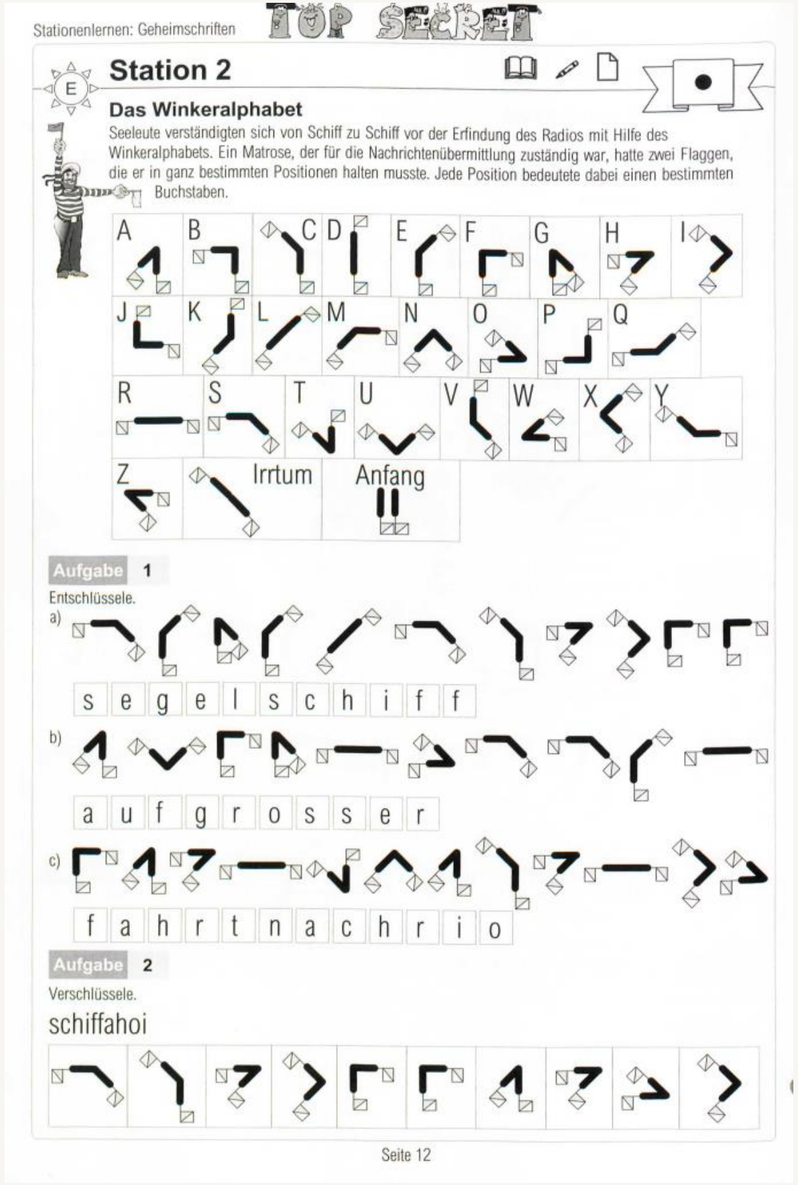
Aufgabe 2

Verschlüssele.

schiffahoi

Stationenlernen Geheimschriften / TOP SECRET! – Best.-Nr. 11 752

Seite 11



Stationenlernen: Geheimschriften TOP SECRET

Station 2

Das Winkeralphabet

Seeleute verständigten sich von Schiff zu Schiff vor der Erfindung des Radios mit Hilfe des Winkeralphabets. Ein Matrose, der für die Nachrichtenübermittlung zuständig war, hatte zwei Flaggen, die er in ganz bestimmten Positionen halten musste. Jede Position bedeutete dabei einen bestimmten Buchstaben.

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 Irrtum Anfang

Aufgabe 1

Entschlüssele.

a) s e g e l s c h i f f

b) a u f g r o s s e r

c) f a h r t n a c h r i o

Aufgabe 2

Verschlüssele.

schiffahoi

Seite 12

DIE BEFREIUNGSMISSIONSSTUNDE

Die Rollen

- Gruppenleiter/ Gruppenleiterin
- Schriftführer/ Schriftführerin
- Zeitwächter/ Zeitwächterin
- Läufer/ Läuferin
- Reine Seele

DIE BEFREIUNGSMISSIONSSTUNDE

Die Gruppen

Bundeskriminalamt

DIE BEFREIUNGSMISSIONSSTUNDE

Das Missionsleitheft

DIE BEFREIUNGSMISSIONSSTUNDE

Das Missionsleitheft

Pi, Bi und Shi wurden von den Illimunaten entführt. Ihr habt 25 Minuten Zeit die Mission zu absolvieren, bevor die drei gefoltert und anschließend ermordet werden.

!!!WICHTIG!!!

- ➔ Bearbeitet die einzelnen Missionen in der Reihenfolge, in der sie angegeben sind.
- ➔ Im Anhang befinden sich Materialien, die ihr zum Lösen der Rätsel gebrauchen könntet. Setzt sie weise ein.
- ➔ Arbeitet im Team!

Teilt euch folgende Zuständigkeitsbereiche zu:

- MissionsleiterIn: _____
- SchriftführerIn: _____
- ZeitwächterIn: _____
- LäuferIn: _____
- reine Seele: _____

Mit vereinten Kräften könnt ihr Pi, Bi und Shi befreien. Viel Erfolg!

DIE BEFREIUNGSMISSIONSSTUNDE

MISSION 1

IHRB ENÖ TIGTDI ESCH ABLO NENUM MERD
REI

Lösung:

_____

MISSION 2

VERWENDET DIE RICHTIGE SCHABLONE.

A	T	I	E	S	E
L	E	A	U	R	P
N	O	Ä	L	S	C
Ö	T	H	T	S	T
E	K	S	E	T	D
T	A	L	.	D	R

Lösung:

_____
_____

MISSION 3

Für das bloße Auge ist der wahre
Inhalt nicht zu erschließen.

Lösung:

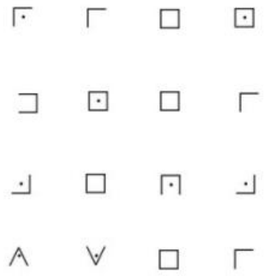
_____

_____

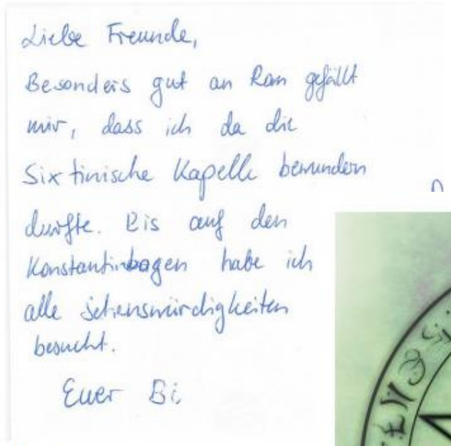
Tauchen Sie ein - Machen Sie sich!

MISSION 4

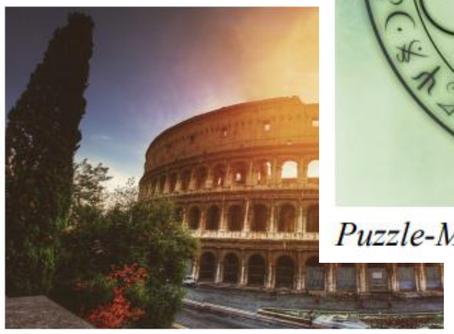
Ihr wisst was zu tun ist!



DIE BEFREIUNGSMISSIONSSTUNDE


Liebe Freunde,
Besonders gut an Rom gefällt mir, dass ich da die Sixtinische Kapelle bewundern durfte. Bis auf den Konstantinbogen habe ich alle Sehenswürdigkeiten besucht.
Euer Bi

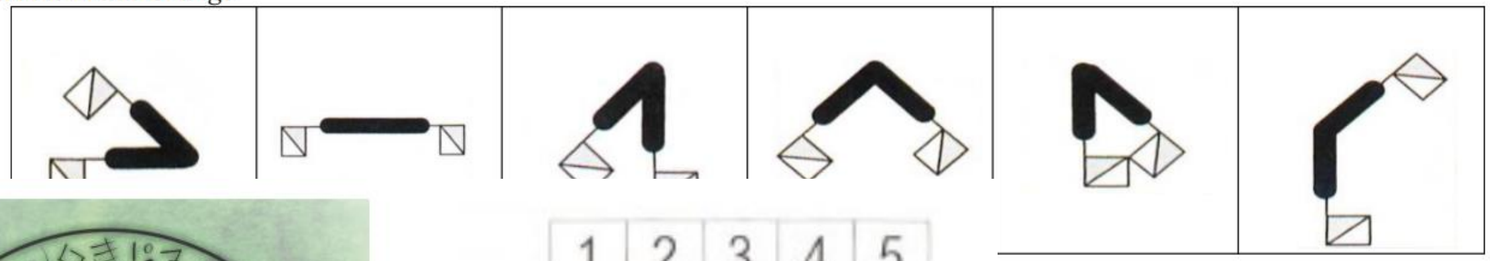
Postkartentext



Postkartenmotiv

Puzzle-Motiv

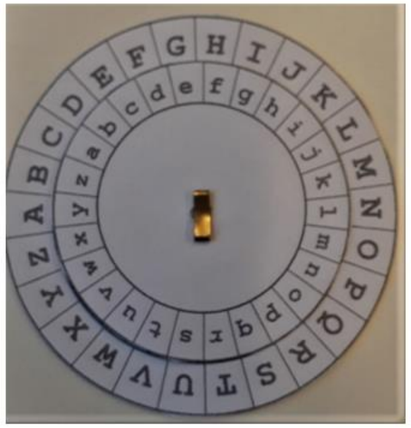
Winker-Text: Orange



Winkerübersicht

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

Polybios-Zahlencode

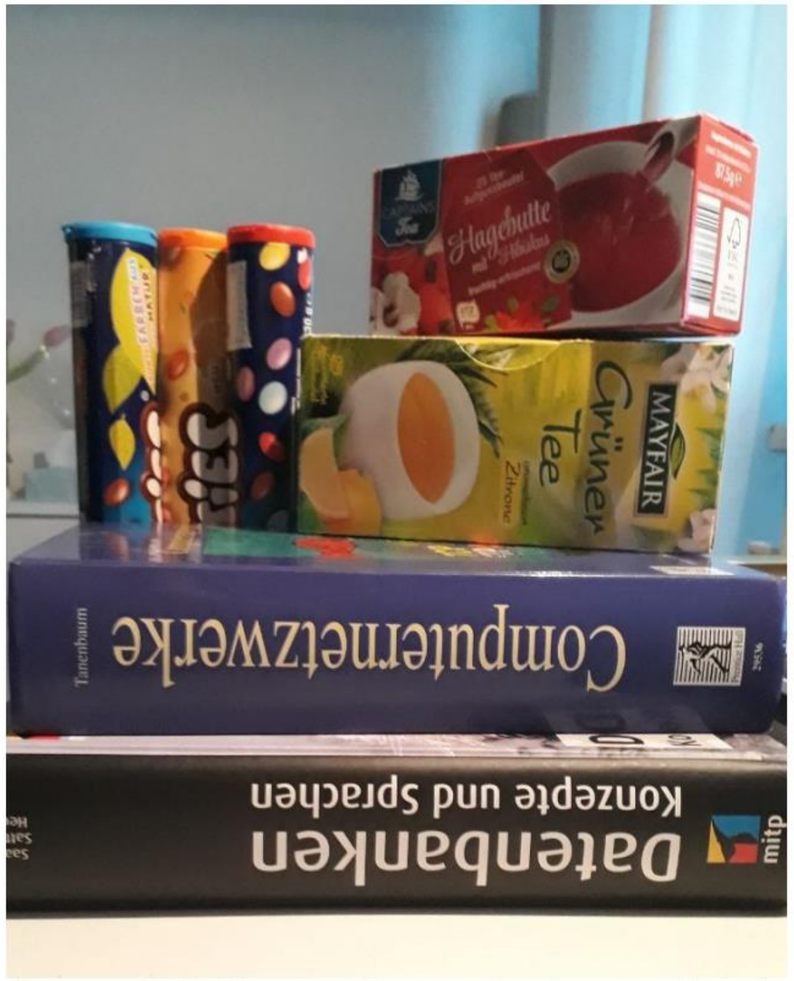


Cäsar-Scheibe

Das Textband

DIE BEFREIUNGSMISSIONSSTUNDE

Truhe, Schlösser, Füllung, Pi, Bi und Shi



Gegenstände, die Hinweise verbergen und im Raum verteilt werden

DIE BEFREIUNGSMISSIONSSTUNDE

Materialideen

- unsichtbare Stifte mit Leuchter
- selbstgebastelte Puzzles
- Postkarten
- Teeverpackungen
- Smartieverpackungen (Skytale)
- Eisstiele
- Bücher
- Luftballons
- Schatztruhe
- Süßigkeiten
- zu rettende Figuren
- Haspe
- (Zahlen-)Schlösser

DIE BEFREIUNGSMISSIONSSTUNDE

Die Lehrersicht

Rätsel	Kurzbeschreibung	Lösung	Hilfsmittel
Zufälliges Trennen	Die SuS verbinden den Textausschnitt und setzen die Leerzeichen an den richtigen Stellen.	Ihr benötigt die Schablone Nummer drei.	6 Schablonen
Schablone	Die SuS wählen die richtige Schablone für das Rätsel aus und legen sie entsprechend an. Drehen müssen sie sie auch.	Leuchtet die Postkarte an. Löst das Rätsel.	6 Schablonen
unsichtbare Schrift	Die beschriebene Seite der Postkarte muss mit dem UV-Stift angeleuchtet werden, um die markierten Buchstaben identifizieren zu können.	Buch Datenbanken	Postkarte, UV-Licht, Buch Datenbanken
Freimaurer	Mit der Freimaurer-Symbol-Übersicht, die sich im Buch befand, entschlüsseln die SuS das letzte Rätsel.	Vier drei neun zwei 4392	Freimaurer-Symbol-Übersicht Schloss mit blauem Punkt

DIE BEFREIUNGSMISSIONSSTUNDE REFLEXION

Positioniere dich.

Ich stimme zu.

Ich stimme nicht zu.

DIGITALE SPURENSUCHE

Entpacken/ Öffnen Sie den Ordner “Digitale Spurensuche”.

DIGITALE SPURENSUCHE

Vorletzte Nacht gab es in Rostock einen Stromausfall. Diesen hat ein Hacker verursacht. Detektiv Leuchte, der mit dem Fall beauftragt war, ist spurlos verschwunden. Seine verschlüsselten Unterlagen hat er jedoch dagelassen. Finde heraus **WO** sich der Hacker versteckt hält, um den nächsten Hackangriff zu verhindern.

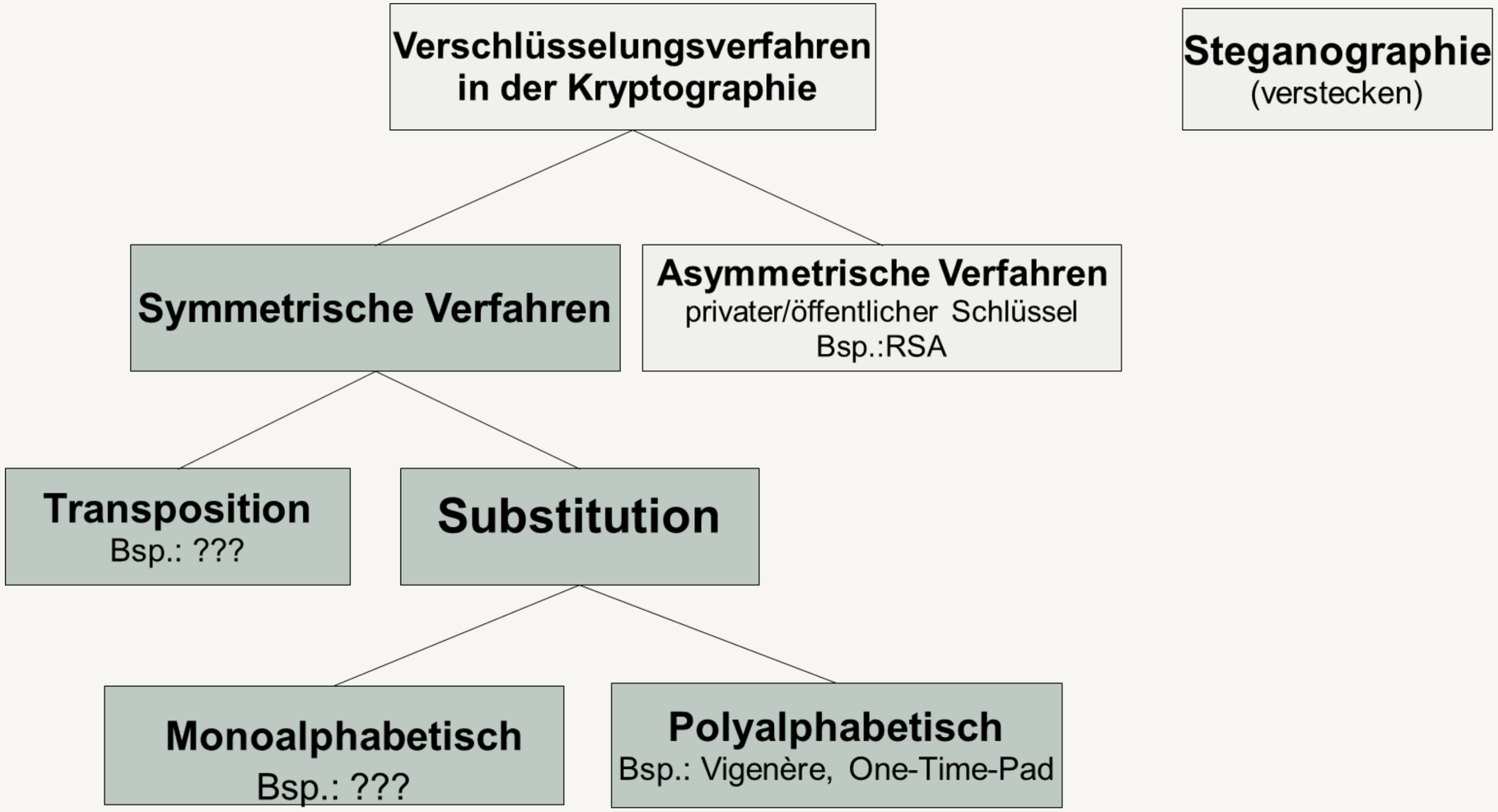
Vergiss nicht: Die Zeit rennt! Start ist bei 1. Hinweis.pdf mit dem Passwort „Turing”.

Sie haben den Hacker gefunden. Gute Arbeit!

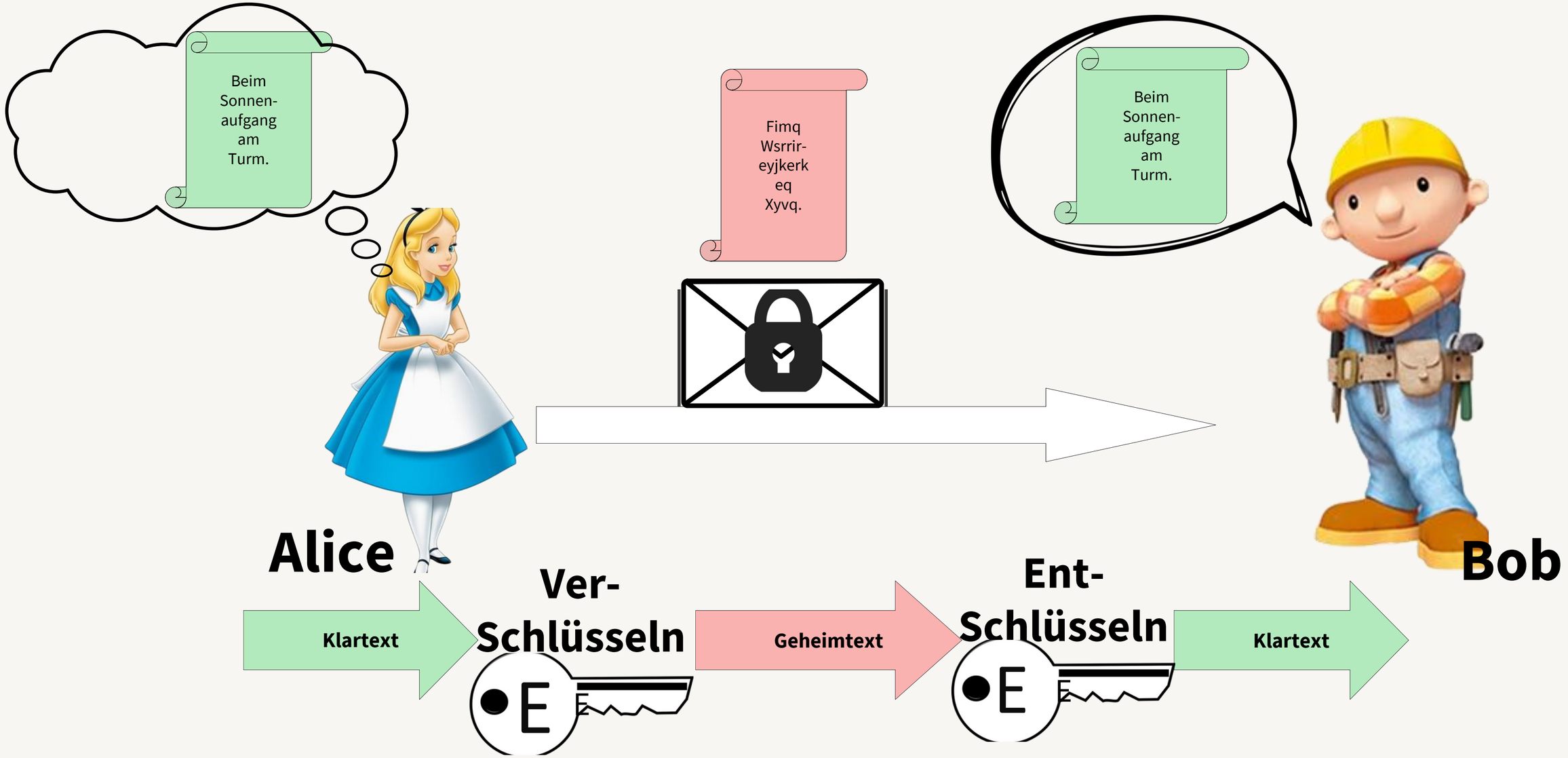
Finde den Hacker
Digitale Spurensuche

Runde	Rätsel	Lösungstext	Material
1	Polybios Morse Caesar	Das Passwort für Brief1 ist der Name des Informatikers, der das CPYNET entwickelte. → **Tomlinson**	Informatiker-Akten 1. Hinweise. pdf (passwort = Turing) Übersetzungstabellen (Polybios, Morse, Zeichen, Freimaurer, ...)
2	Weißer Text	P.S.: Währen des Spaziergangs in Rostock habe ich echt schöne Bilder aufgenommen. Schau dir die mal genau an. Nutze bei Auffälligkeiten den wxHexEditor.	Brief1.odt
3	Bilder	Jetzt nicht durchdrehen. Für das Dokument Schablone.draw ist das Passwort „**JohnVonNeumann**“.	HexEditor Bilder
4	Schablone	Das Kreuzwortpasswort ist **MURRAYHOPPER!**	Schablone.draw
5	Anagramm	**Anfangsbuchstaben**	Kreuzwort.pdf
6	Postkarte	Passwort: Ada Lovelace Verbinde jeden zweiten Ort auf der Karte.	Postkarte.pdf
7	Karte	Kreuz auf Landesamt für Gesundes und Soziales	Karte-Rostock.png Zeichenprogramm

SYSTEMATIK DER VERSCHLÜSSELUNGSVERFAHREN

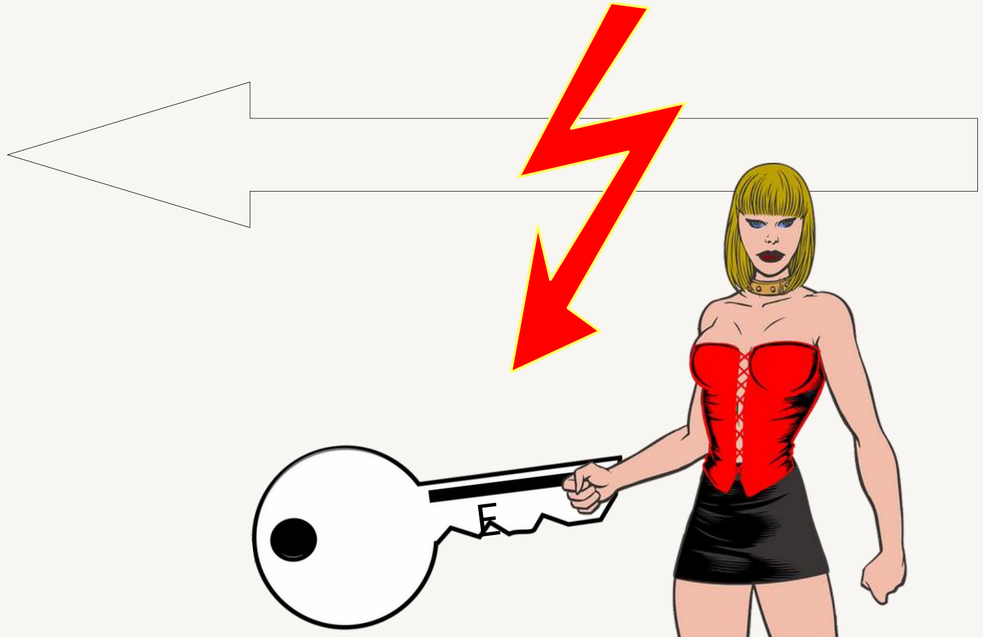


DIE SYMMETRISCHE VERSCHLÜSSELUNG



DIE SYMMETRISCHE VERSCHLÜSSELUNG

Alice



Eve

Bob

Von nun an nutzen wir nur noch die asymmetrische Verschlüsselung!

Alice

ROLLENSPIEL

DIE ROLLEN

Alice

Bob

Eve

Schlüsselmacher

Bote

Erzähler

AUFBAUENDE FRAGE

WIE MÜSSTE ALICE IHRE ANTWORT VERSCHICKEN, SODASS SIE SICHER BEI BOB ANKOMMT?

Erzählertext

ALICE möchte ganz sicher gehen und nutzt die asymmetrische Verschlüsselung beim Nachrichtenaustausch.
ALICE veranlasst den SCHLÜSSELMACHER ihr zwei Arten von Schlüsseln anzufertigen.
Zum einen fertigt der SCHLÜSSELMACHER Alice einen privaten Schlüssel an und überreicht ihr diesen.
ALICE versteckt den Schlüssel sicher bei sich.

Die zweite Art Schlüssel, den der SCHLÜSSELMACHER anfertigt, ist der öffentliche Schlüssel.
Davon fertigt er mehrere Exemplare an und überreicht sie ALICE.

ALICE verteilt nun ihre öffentlichen Schlüssel an BOB und zwei weitere Personen.

BOB verfasst eine Nachricht, indem er einen Text auf Papier schreibt.
Diese Nachricht möchte BOB verschlüsseln.
Hierfür legt BOB seinen beschriebenen Zettel in die Box und verschließt die Box mit seinem öffentlichen Schlüssel.

Kurz nach dem verschlüsseln fällt BOB auf, dass er den Anhang vergessen hat.
Er versucht die Box zu öffnen, doch vergeblich. Die Nachricht kann nicht mehr entschlüsselt werden.

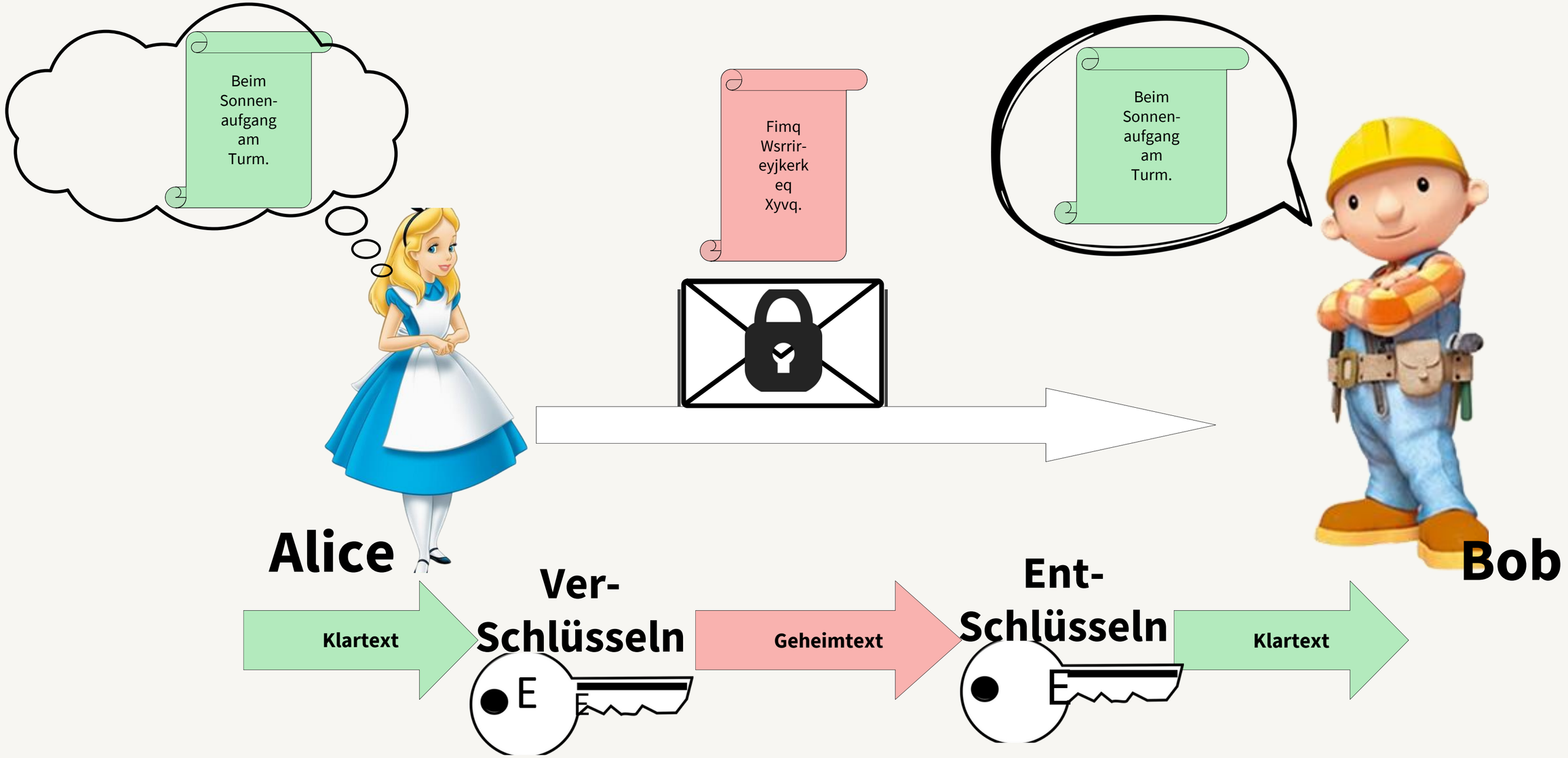
Also übergibt BOB die Nachricht dem BOTEN und versendet die Nachricht.
Auf dem Weg des BOTEN zu Alice wird der BOTE von EVE überfallen und EVE erhält die verschlüsselte Nachricht.
EVE versucht die Nachricht zu entschlüsseln. Doch es gelingt ihr nicht.

Dem BOTEN gelingt es die Nachricht wieder an sich zu reißen.
Er setzt seine Reise zu ALICE fort.
Sobald ALICE ihre Nachricht erhalten hat, zückt ALICE ihren privaten Schlüssel und entschlüsselt Bobs Nachricht und liest den Inhalt.

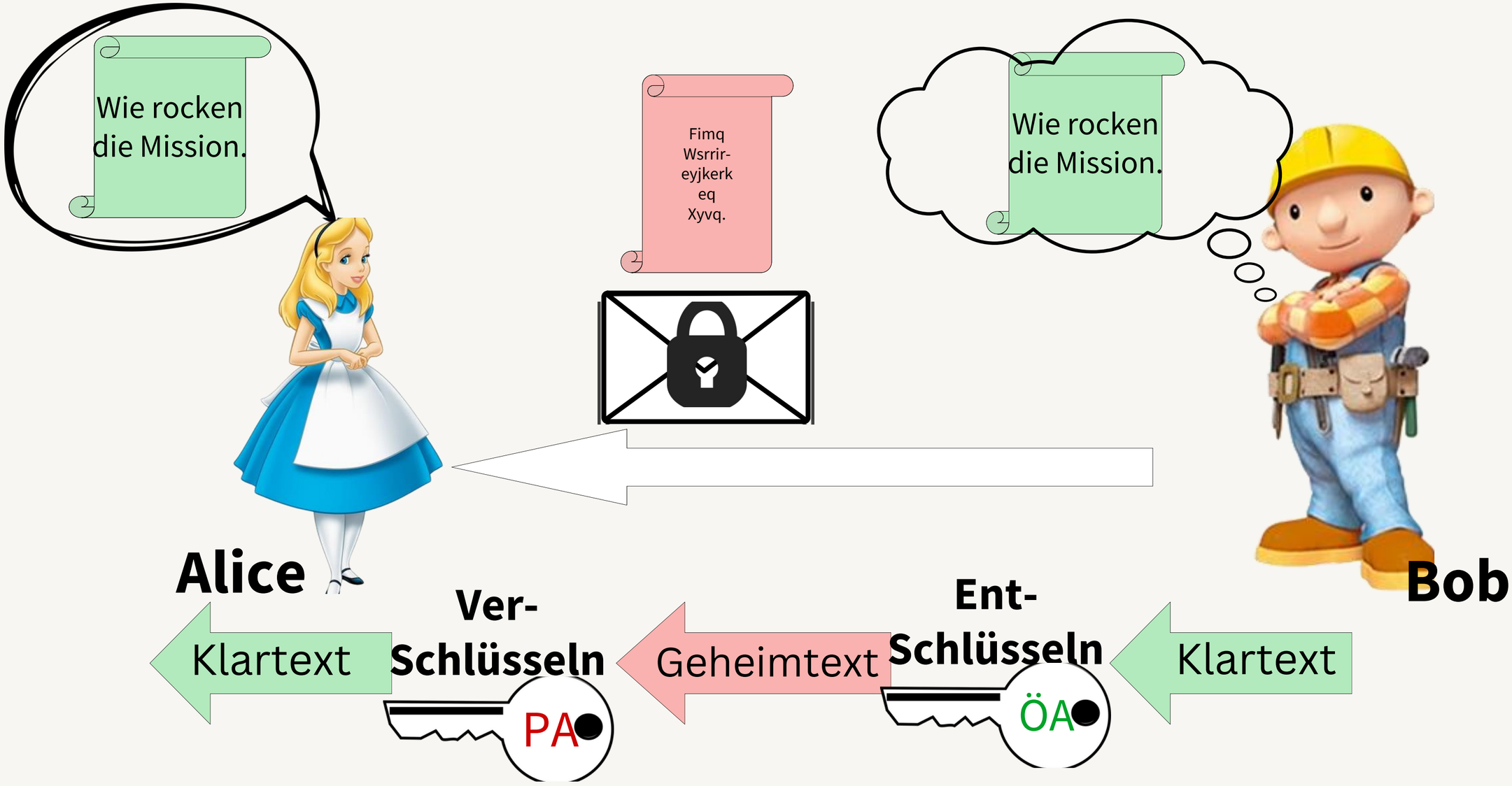
DIE REQUISITEN

- Rollenbezeichnungen (Bob, Alice, Eve, Schlüsselmacher, Bote, Erzähler)
- 3 Schlösser + 1 Schlüssel
- verschließbare Box (2 Schlüsselringe)
- Stück Papier + Stift

DIE SYMMETRISCHE VERSCHLÜSSELUNG



DIE ASYMMETRISCHE VERSCHLÜSSELUNG



INPSIRATIONEN UND LINKS

INPSIRATIONEN UND LINKS

- Heft: Schmidt, H.-J. (2016, 2. Auflage): **Stationenlernen Geheimschriften. Top Secret!**. Köln: Kohl-Verlag.
- Video von Stefan Müller: **“Brickscience TV - Kryptographie ("Fast Forward Science 2017")”** (2017), unter: https://www.youtube.com/watch?v=Ntt-hz_Dvo4
- **Krypto im Advent**: https://krypto-im-advent.de/
- **Serie Blindspot** (2015) Staffel 1, Folge 2 “Die Narbe im Nacken”, 6:08 - 7:20 min --> Vigenère-Verschlüsselung prüfen
- Matheprisma: **RSA Asymmetrie** (online, interaktiv), unter: https://www.matheprisma.uni-wuppertal.de/Module/RSA/pages/node3.htm

INPSIRATIONEN UND LINKS

- weiteres **Escape-Spiel: Fall 181120**, unter: https://www.cs.uni-potsdam.de/room-x/files/Fall181120/downloads.html
- weiteres **Escape-Spiel: Die Suche nach dem verlorenen Schatz - Kryptographie zum Anfassen** - RWTH Aachen Universität, unter: https://www.infosphere.rwth-aachen.de/cms/infosphere/Angebote/InfoSphere-Workshops/~bhsrdd/Schatzsuche/
- Stationsarbeit: **Spion Camp** - Uni Wuppertal, unter: https://ddi.uni-wuppertal.de/web/website/index-ddi.html?navi=materialien&main=spioncamp
- Unterrichtsreihe: **E-Mail (nur?) für dich** - Uni Beyreuth, unter: https://medienwissenschaft.uni-bayreuth.de/inik/entwuerfe/email-nur-fuer-dich/