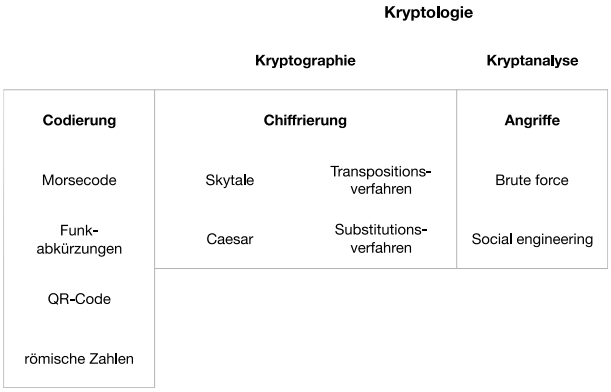
Transparenter Verlauf

EduBreakout Kryptologie

Ablauf

Phase/ (Zeit) /Methode	Beschreibung/ Inhalt	Material/ Medien
2“	Aufteilen des Kurses in (drei) Gruppen kurze Erläuterung des Auftrags	im Raum verteiltes Breakout-Material
70“	Breakout	dito
18“	Auswertung Strukturieren, Einführen von Fachbegriffen	Tafel o. ä.

Mögliches Tafelbild



Benötigtes Material für drei Gruppen

3 Werkzeugkisten

3 Verriegelungshaspen

3 Caesar-Scheiben

3 Flaschen und Skytale-Streifen

Haftnotizen

ausgedruckte Blätter für die drei Gruppen

3 Calliope

1 Computer mit vorbereiteten Accounts (s. u.)

9 Schlösser, z. B.: 3 Schlösser mit 5 Buchstaben

2 Schlösser mit 5-stelligem Zahlencode

1 Master Lock One

Transparenter Verlauf

Hinweise

Die verwendeten Codes sind authentische Codes aus dem (Morse-)Funkverkehr. In den verlinkten Webdokumenten sind weitere Codes aufgeführt, die unter lizensierten Funkamateuren verwendet werden:

Telegrafieabkürzungen beim DARC: https://www.darc.de/der-club/referate/ajw/lehrgang-bv/bv03/

Abkürzungen im Amateurfunk beim DARC: https://www.darc.de/der-club/referate/ajw/lehrgang-bv/bv04/#teil2

Es kommen sowohl Codes als auch Chiffren vor, so dass der Unterschied leicht herausgearbeitet werden kann. Auftretende **Codes** sind:

Morsecode, römische Zahlen	stellen Information für das Übertragungsmedium dar
QR-Code	mit Hilfe redundanter Information wird Fehlertoleranz erreicht
Funkabkürzungen	erleichtern den Betriebsablauf, verschleiern aber die Information nicht

Bei den Funkabkürzungen ergibt sich der Gesprächsanlass, dass Codes frei definiert werden können. Während die auf dem Arbeitsblatt hinter den Q-Gruppen verwendeten größtenteils als Abkürzungen erkannt werden können, gibt es mit den Q-Gruppen eine große Zahl weiterer gebräuchlicher Codes, die nicht alle ableitbar sind. Evtl. sind den SuS auch andere Konnotationen des im Funkverkehr völlig unverfänglichen Codes 88 bekannt. https://de.wikipedia.org/wiki/Achtundachtzig

Auftretende **Chiffren** sind:

Caesar	einfaches Substitutionsverfahren
Skytale	einfaches Transpositionsverfahren

Die Schülerinne und Schüler müssen verschiedene **Angriffe** auf die Rätsel nutzen. Dazu gehören das **Dechiffrieren** der Skytale und des Caesar-Textes, der **Brute-Force-Angriff**, da ein Buchstabe für das fünfstellige Schloss fehlt und das Herausfinden des Passworts für den Account am Computer. Letzteres bietet, ggf. in einer späteren Stunde, einen Gesprächsanlass zum sicheren Umgang mit Passwörtern und zum Social Engineering.

Computer

Ein Computer im Raum muss präpariert werden, am besten ein sonst nicht dort vorhandener, so dass deutlich wird, dass er zum Spiel gehört. Unter der Tastatur sind (bspw. drei farbige) Klebenotizen anzubringen mit den Kennwörtern für die Accounts. In jedem Account ist eine Einkaufsliste zu finden, z. B. in der macOS-App Erinnerungen oder einer Textdatei. Diese enthält einen Artikel, der einen Lösungsbuchstaben liefert, vgl. Übersicht der Schlösser.

Bezugsquellen

Sämtliches Material ist im Baumarkt bzw. im einschlägigen Online-Handel leicht zu besorgen. Bei der Suche nach „Hasp“ bzw. „Verriegelungshaspe“ werden dabei interessante Schlösser gleich mit angeboten.

Anpassungen

Die verfügbaren Schlösser erfordern ggf. eine leichte Anpassung der Rätsel. Die korrekten Lösungen sollten unbedingt in einem Blatt wie der Übersicht dokumentiert werden, damit der Bolzenschneider in der Werkstatt bleiben kann.

Viel Spaß!