Wissensfabrik
Mehr Wissen. Mehr Können. Mehr Zukunft.

IT2School

Gemeinsam IT entdecken

Modul A2 – Kryptologie

Kryptologie

Eine Entwicklung von

OFFIS
INSTITUT FÜR INFORMATIK

In Kooperation mit

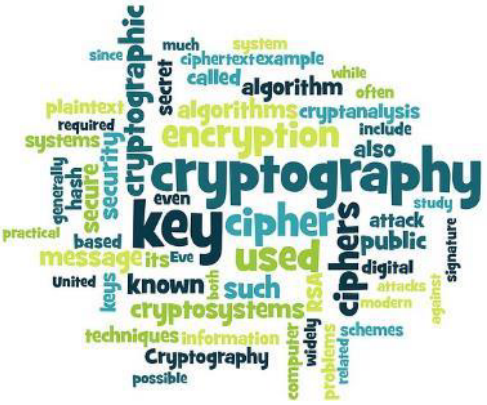
Carl von Ossietzky
Universität
Oldenburg

Im Auftrag der

Wissensfabrik
Mehr Wissen. Mehr Können. Mehr Zukunft.

Inhalt

1 Kryptologie



In diesem Modul befassen sich die Schülerinnen und Schüler mit dem Ver- und Entschlüssel von Informationen. Dabei werden Sicherheitsaspekte bei Kommunikationsvorgängen im Alltag aufgezeigt und verschiedene Verfahren zur Verschlüsselung aus der Vergangenheit bis zur heutigen Moderne vorgestellt.

In Anlehnung an ein „Text-Adventure“ erhalten die Schülerinnen und Schüler einen Überblick über verschiedene Verschlüsselungsverfahren. Sie müssen dabei kleinere Aufgaben lösen, während sich im Lauf der Zeit die Geschichte entfaltet.

Zum Abschluss können die Schülerinnen und Schüler die eigene Veröffentlichung von persönlichen Informationen sowie deren Kommunikation reflektieren und sich entsprechend absichern.

Lernfeld/Cluster:	Kommunikation erkunden	
Zielgruppe/Klassenstufe:		4. bis 5. Klasse
	X	6. bis 7. Klasse
	X	8. bis 10. Klasse
	X	11. bis 12. Klasse
Geschätzter Zeitaufwand:	6 Einzelstunden	
Lernziele:	• Bedeutung von Verschlüsselung im Alltag und Arbeitswelt kennenlernen • Kryptographische und kryptoanalytische Verfahren kennenlernen • Ausgewählte Verfahren anwenden und „knacken“ können • Eigenen Umgang mit persönlichen Informationen reflektieren und anschließend schützen	
Vorkenntnisse der Schülerinnen und Schüler:	Keine	
Vorkenntnisse der/des Lehrenden:	Keine	
Vorkenntnisse der Unternehmensvertreterin/des Unternehmensvertreters:	Keine	
Sonstige Voraussetzungen:	Keine	

2 Warum gibt es das Modul?

Die Geschichte der Kryptologie ist eine alte Geschichte, die bis ins alte Ägypten und Griechenland zurückgeht. Obwohl sie in den Anfängen hauptsächlich für militärische Zwecke genutzt wurde, fand sie trotzdem den Weg in unseren Alltag.

Täglich haben wir es mit Verschlüsselung zu tun, bewusst oder unbewusst: Beim Schreiben einer WhatsApp-Nachricht, beim Online-Banking, beim Fernsehen von Bezahl-Sendern oder beim Bezahlen mit der EC-Karte. Dass in diesen Beispielen nicht jeder die übermittelten Daten einfach so lesen soll, ist sofort ersichtlich.

Für Unternehmen ist das Thema Verschlüsselung in Zeiten von Betriebsspionage und Cyberkriminalität von besonderer Bedeutung. Laut dem Bundeskriminalamt beläuft sich der jährliche Schaden in Deutschland auf ca. 50 Milliarden Euro, wobei von einer hohen Dunkelziffer ausgegangen wird. Sensible Inhalte, wie personenbezogene Daten sowie geistiges Eigentum müssen daher auch in Betrieben und Wirtschaftunternehmen geschützt werden.

Durch die NSA-Enthüllungen der letzten Jahre wurde das Thema der Verschlüsselung besonders präsent und immer mehr Menschen fangen an darüber nachzudenken, was mit ihren Daten passiert oder wie sie diese schützen können.

3 Ziele des Moduls

- Bedeutung von Verschlüsselung im Alltag und Arbeitswelt kennenlernen.
- Kryptographische und kryptoanalytische Verfahren kennenlernen.
- Ausgewählte Verfahren anwenden und „knacken“ können.
- Eigenen Umgang mit persönlichen Informationen reflektieren und anschließend schützen.

4 Die Rolle der Unternehmensvertreterin/des Unternehmensvertreters

Im Modul *A2 – Kryptologie* hat die Unternehmensvertreterin/der Unternehmensvertreter mehrere Möglichkeiten aktiv mitzuwirken. Hier einige Anregungen:

- Special-Guest: Kann über eigene Sicherheitsaspekte im Unternehmen berichten
- Kann beim Text-Adventure mitmachen

5 Inhalte des Moduls

Im Rahmen dieses Moduls geht es um *Geheime Kommunikation*, dabei werden die Begriffe *Kryptologie*, *Steganografie* sowie *Codierung* näher betrachtet und klar definiert. Als **Kryptologie** wird die Wissenschaft der Informationssicherheit bezeichnet. Dabei unterteilt sich diese in zwei Unterbereiche auf: Die **Kryptographie** beschäftigt sich mit der Verschlüsselung von Informationen und die **Kryptoanalyse** mit deren Entschlüsselung.

Die Geschichte der Kryptographie ist bereits sehr alt und spielte insbesondere für das Militär eine große Rolle. Die historischen Verschlüssselungsvarianten finden heute keine Verwendung mehr, aber anhand der Beispiele lassen sich die Grundlagen verdeutlichen.

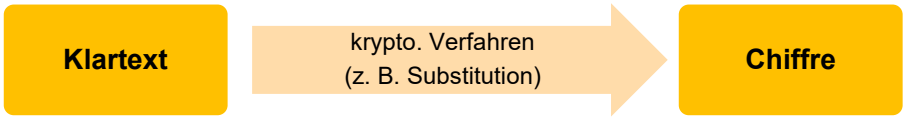
Die in der Kryptographie gebräuchlichen Verfahren nennt man **Substitution** und **Transposition**.

Bei der sogenannten **Transposition** werden Buchstaben oder Wörter im Klartext verschoben, so dass ein Sinnzusammenhang nicht direkt erkennbar wird bzw. der Klartext nicht so leicht lesbar ist. Als ein einfaches historisches Beispiel ist die griechische Skytale zu nennen. Mit Hilfe eines Holzstabes verschlüsselten die Griechen um ca. 400 v. Chr. ihre Nachrichten. Dabei wurde ein Papier- oder Lederstreifen um einen Holzstab gewickelt und dann darauf die Nachricht verfasst. Der Durchmesser des Skytales war der entscheidende Schlüssel zum entschlüsseln der Chiffre.

Skytale
https://de.wikipedia.org/wiki/Skytale

Ein weiteres Beseispiel ist die Pallisaden- oder Gartenzaun-Chiffre. Die Buchstaben des Textes werden abwechselnd auf zwei Zeilen geschrieben, so dass der erste auf der oberen, der zweite auf der unteren, der dritte Buchstabe wieder auf der oberen Zeile steht und so weiter. Anschließend fügt man das Ganze zeilenweise wieder zusammen.

Bei der **Substitution** werden einzelne oder mehrere Buchstaben oder ganze Wörter innerhalb eines *Klartextes* (dem Text bzw. der Information vor Anwendung eines kryptographischen Verfahrens) vertauscht, wodurch aus diesem die *Chiffre* entsteht.



Eines der bekanntesten Beispiele ist die Caesar-Verschlüsselung, die schon in *Modul B1 – Vom Blinzeln zum Verschlüsseln* behandelt wurde. Die Nachricht wird verschlüsselt indem jeder Buchstabe durch einen Buchstaben ersetzt wird, der um eine bestimmte Stelle im Alphabet versetzt wurde. Bei einer Verschiebung von 3 Stellen wird beispielsweise der Buchstabe A zu D usw.

Ein ähnliches Verfahren nutzten die Bewohner von Palestina in der Zeit von ca. 600-500 v. Chr. Bei der sogenannten *Altbash-Verschlüsselung* wurde der erste Buchstabe des Alphabets mit dem letzten Buchstaben, der Zweite mit dem Vorletzten usw. ersetzt (A=Z; B=Y,…)

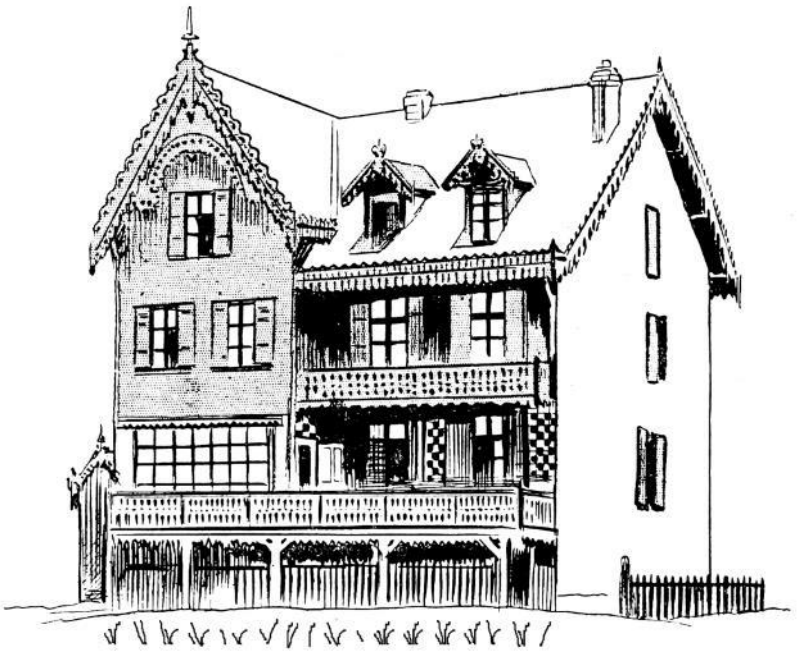
Um ca. 755 n. Chr. herum gelang es dem arabischen Philosophen Abu-Yusuf Ya'qub ibn Ishaq al-Kindi als erster ein kryptoanalytisches Verfahren zum Knacken des Subsitutionsverfahrens zu Beschreiben: **die Häufigkeitsanalyse.** Hierbei wird eine Chiffre danach untersucht, welche Symbole, Buchstaben oder Zahlen besonders häufig vorkommen. Anschließend wird geprüft, ob die am häufigsten vorkommenden Buchstaben bzw. Symbole aus der Chiffre mit den am häufigsten vorkommenden Buchstaben der jeweiligen Sprache bzw. Schrift ersetzt werden können (siehe auch Modul B1).

Anfang der zwanziger Jahre entwickelte Arthur Scherbius als erster eine Maschine zur Codierung, die so genannte *Enigma*. Sie bestand aus mehreren Chiffierungszylindern, die jeweils unterschiedliche Substitutionen innerhalb des Alphabets vornahm. Durch die hohe Anzahl an verschiedenen Walzen und Konfigurationsmöglichkeiten ergaben sich viele

Verschlüsselungsmöglichkeiten, weshalb sie zu damaliger Zeit als sehr sicher galt. Die Deutschen nutzen während des 2. Weltkrieges diese Form der Verschlüsselung. Im Jahr 1940 gelang es Marian Rejewski und Alan Turin die Enigma-Entschlüsselung zu knacken, wodurch sie den Ausgang des 2. Weltkrieges entscheidend beeinflussten.[1]

Die **Codierung** wird verwendet, um Daten für eine entsprechende Anwendung in ein geeignetes Format zu bringen. Innerhalb der Basismodule haben wir schon Codes kennengelernt. Beispielsweise in Modul B1 den Morsecode oder im Modul B3 den Bar- und QR-Code. Mit Kenntnis des Codes ist die Entschlüsselung des Inhalts unproblematisch, hat man diesen nicht, hilft manchmal nur ein Zufallsfund, wie beispielsweise der Stein von Rosetta, der bei der Dechiffrierung der ägyptischen Hieroglyphen eine entscheidende Rolle spielte.

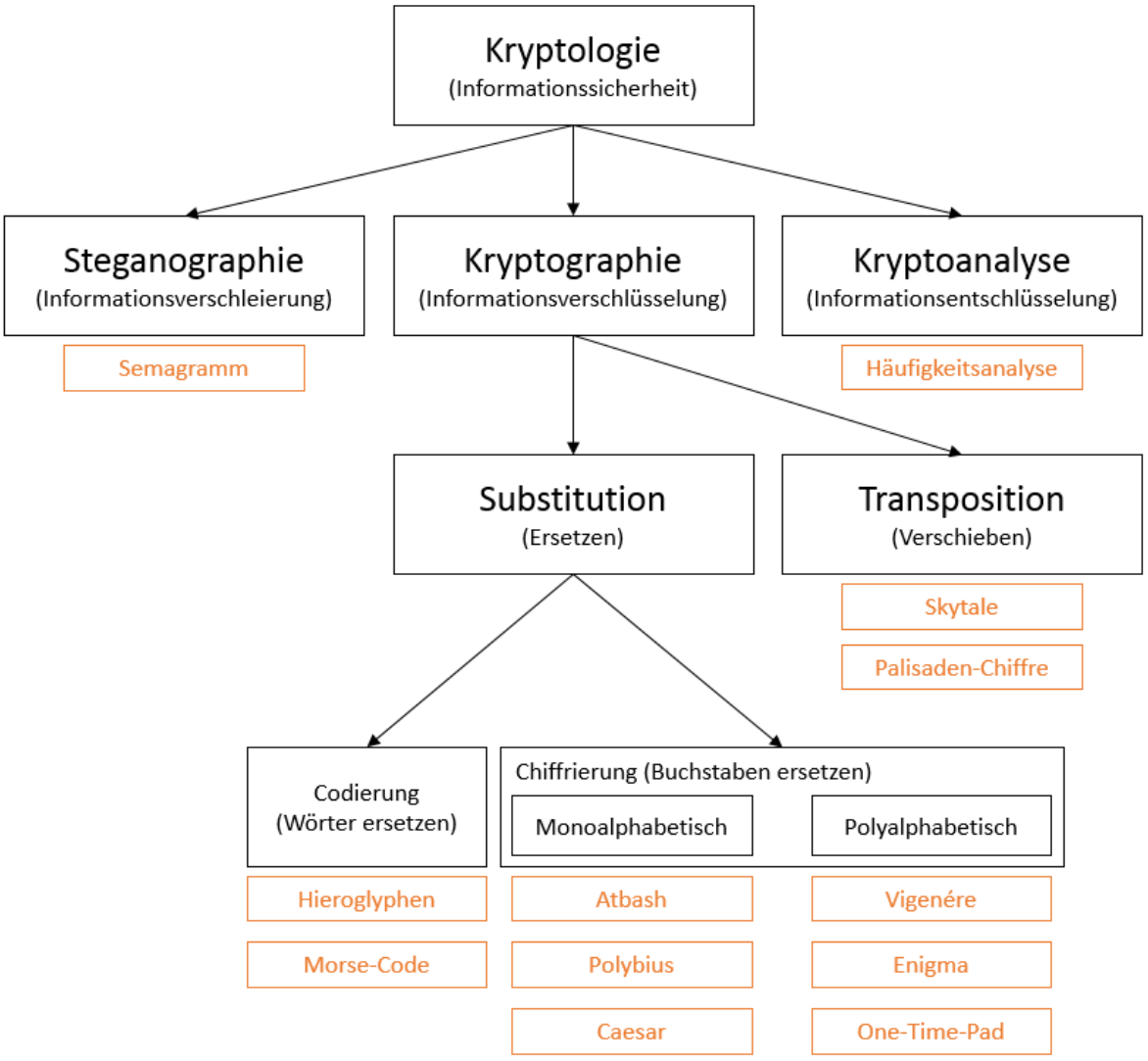
Bei der **Steganographie** steht die Verschleierung der Informationen im Vordergrund. Es gibt verschiedene Arten von steganographischen Verfahren. Historische und auch eher klassische Beispiele stellen dabei die unsichtbare Tinte (Zitronensaft), doppelte Böden in Paketen oder Briefumschlägen dar. Es gibt aber auch Verfahren, die mit der Sprache und der Codierung der Sprache arbeiten, wie beispielweise Semagramme. Hierbei handelt es sich um Bilder, in denen kleine Details versteckt sind, die allerdings die codierten Geheiminformationen darstellen. Betrachtet man zum Beispiel das folgende Bild, so fällt dem Betrachter die geheime Nachricht nicht direkt auf. Erst wenn man weiß, dass es sich bei den Grashalmen um Morsecode handelt, kann der Betrachter die Nachricht decodieren.



Auch im digitalen Bereich gibt Einsatzgebiete für Semagramme. Innerhalb einer MP3-Audio-Datei oder eines Bildes im JPG-Format lassen sich zusätzliche Bytes einfügen ohne das sich die urspüngliche Melodie oder das Bild ändert.

[1] Hierzu gibt es mehrere Verfilmungen wie zum Beispiel *The Imitation Game* oder die Arte Dokumentation *Wie ein Mathegenie Hitler knackte*.

5.1 Schaubild zur Kryptologie



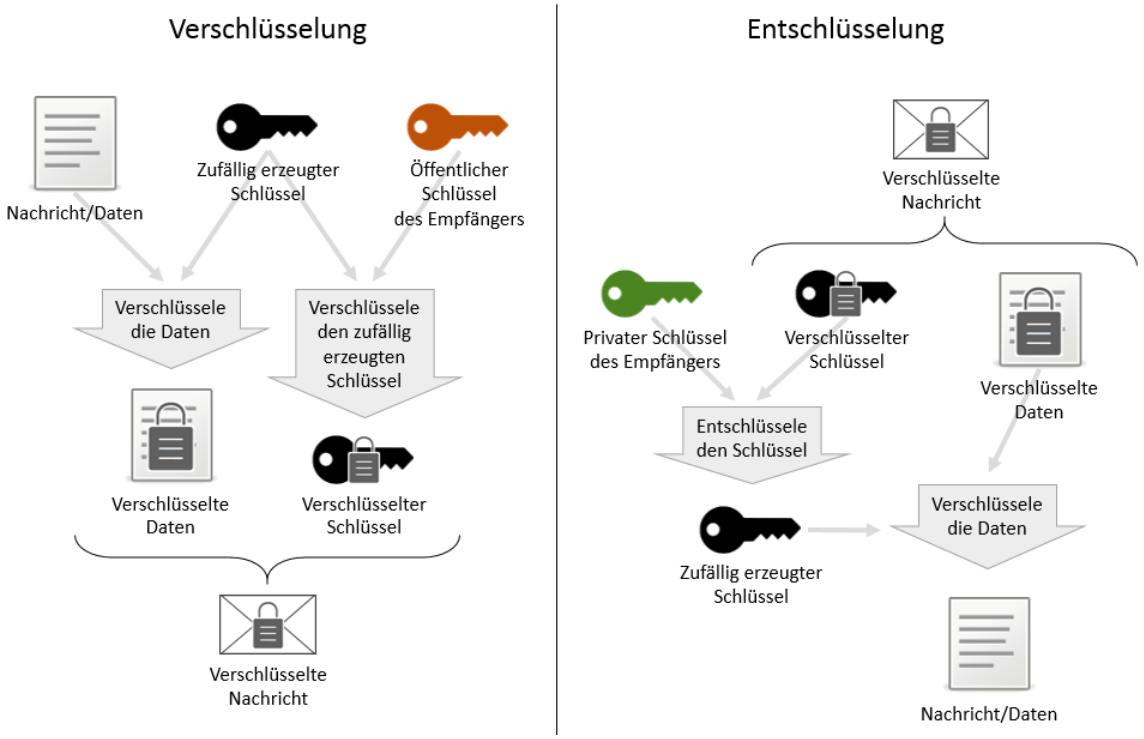
5.2 Moderne Kryptologie

In der heutigen Zeit gibt es immer noch viele verschiedene Arten von Verschlüsselung, bei der allerdings die Mathematik, im Gegensatz zu den historischen Beispielen, eine viel größere Rolle spielt. Aber auch Begriffe wie Public- und Private-Key oder symmetrische und asymetrische Verschlüsselung finden in diesem Zuhammenhang Verwendung.

Wichtig für das Verständnis ist zunächst einmal die Abgrenzung von symmetrischer und asymmetrischer Verschlüsselung. Hierbei werden Verfahren in zwei Gruppen eingeteilt, wobei die uns bekannten Verfahren alle zur Gruppe der symmetrischen Verschlüsselungsverfahren gehören. Bei der symmetrischen Verschlüsselung erfolgt die Ver- und Entschlüsselung mit dem selben Schlüssel bzw. anhand des selben Verfahrens (z.B. Verschiebung des Alphabetes bei Caesar). Anders funktionieren die asymmetrischen Verschlüsselungsverfahren (wie z. B. RSA), bei der zur Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden. Diese unterschiedlichen Schlüssel bei der asymmetrischen Verschlüsselung werden dann auch Public- and Private-Key genannt. Verständlicher wird die asymetrische Verschlüsselung, wenn man sich als Beispiel die Funktionsweise von RSA genauer anschaut.

Die drei Buchstaben von RSA stehen für die Namen Rivest, Shamir und Adleman, die dieses Verfahren 1977 entwickelten. RSA arbeitet mit mathematischen Verfahren der Zahlentheorie und der modularen Arithmethik. Für ein tiefergehendes Verständnis ist daher Wissen über die Division mit Rest und die Kongruenzrelation notwendig. Beides soll hier jedoch nicht weiter vertieft werden, da die eigentliche Funktionsweise zum Verständnis der asymmetrischen Verschlüsselung nicht zwingend erforderlich ist. Entscheidend ist, dass für die Sicherheit des Verfahrens sehr große Primzahlen p und q verwendet werden. Es werden anschließend mit mathematischen Verfahren zwei weitere Zahlen e und d ermittelt. Das Paar (e, pq) bildet dann den öffentlichen Schlüssel und das Paar (d, pq) den privaten Schlüssel. Der öffentliche Schlüssel kann von einer Person veröffentlicht werden, damit andere Personen ihm verschlüsselte Nachrichten zulassen kommen können. Eine Schritt für Schritt-Anleitung und Schaubild zu RSA befindet sich hierzu auch im Arbeitsmaterial V3.7.

Ein hybrides Verfahren der symmetrischen und asymmetrischen Verschlüsselung stellt PGP dar. PGP steht für Pretty Good Privacy und ist ein Programm zur Verschlüsselung und zum Unterschreiben, das von Phil Zimmermann entwickelt wurde und wird häufig bei der Verschlüsselung von E-Mails verwendet. Die erste Version, die1991 entstand, benutzte RSA zum Verschlüsseln von Daten. In den späteren Versionen wird jedoch auf Elgamal als Verschlüsselungsverfahren zurückgegriffen. Um den Aufwand der Verschlüsselung möglichst gering zu halten, werden nicht die gesamten Daten mit einem asymetrischen Verfahren verschlüsselt. Zunächst wird ein zufälliger Schlüssel erzeugt und mit einem asymetrischen Verfahren verschlüsselt. Dieser zufällige Schlüssel dient zur symmetrischen Verschlüsselung der eigentlich Daten. Das folgende Schaubild zeigt dies etwas genauer:



6 Unterrichtliche Umsetzung

Diese Unterrichtsheinheit ist als eine Art „Text-Adventure“ geplant, daher wird sich im Verlauf der Unterrichtsreihe eine Detektivgeschichte entfalten. Als Einstieg und damit sich die Schülerinnen und Schüler die kryptographischen Verfahren spielerisch selbst aneignen, erhalten diese in der ersten Unterrichtsstunde eine E-Mail mit einem verschlüsselten Text.

Damit ist die kryptographische Schnitzeljagd eröffnet und die Schülerinnen und Schüler müssen verschiedene Verschlüsselungen knacken und helfen letztlich, den entführten Pudel Rex zu finden. In wie weit die Schülerinnen und Schülern durch Arbeitsmaterialien unterstützt werden können, liegt bei der Lehrkraft. Vorgesehen ist jedoch, dass diese sich selbst über die kryptographischen Verfahren informieren und ihren Wissenszuwachs kontinuierlich mittels einer MindMap darstellen. Ziel ist es, die Beziehungen zu den einzelnen Begriffen und Konzepten herzustellen.

Im Anschluss an die Detektivgeschichte befassen sich die Schülerinnen und Schüler mit heutigen Verschlüsselungsverfahren und den Fragestellungen zur Datensicherheit. Hierfür empfehlen wir zum einen, sichere Kommunikationswege im Alltag (siehe Abschnitt 6.1) der Schülerinnen und Schüler aufzuzeigen sowie deren Nutzen und Bedeutung zu erarbeiten. Zum anderen sollte auch die praktische Anwendung von Verschlüsselungen, zum Beispiel in Form von Datei- oder E-Mailverschlüsselung thematisiert und durchgeführt werden. Hierfür bietet sich unter anderem das Video „Men in Grey“ (https://criticalengineering.org/projects/men-in-grey) an, das zeigt, wie eine Gruppe von Datenschutzaktivisten die Daten eines öffentlichen WLAN abgreifen und anschließend über einen Monitor und Sprachausgabe zurück an ihre Umwelt wiedergeben können.

6.1 Datensicherheit im Alltag

Nach dem Text-Adventure und der Auseinandersetzung mit den heutigen Verschlüsselungsverfahren, besprechen und reflektieren die Schülerinnen und Schüler aktuelle Beispiele für Sicherheitslücken und Absicherung von Diensten anhand von lebensweltorientierten Themen wie z.B. WhatsApp. Der beliebte Messenger bietet seit einiger Zeit eine Ende-zu-Ende Verschlüsselung an, d.h. das lediglich Sender und Empfänger in der Lage sind, die Nachrichten zu Entschlüsseln.

Die folgende Auswahl zeigt weitere Beispiele aus dem Alltag:

Das Onlinebanking ist ein typisches Beispiel für eine Verschlüsselung der Kommunikation zwischen Browser des Kunden und Webserver der Bank. Beim Aufruf und dem späteren Anmelden sowie den anschließenden Tätigkeiten (Überweisungen etc.) werden sensible Daten ausgetauscht. Damit dieser Austausch möglichst sicher ist, wird auf das Protokoll HTTPS zurückgegriffen. Anders als das normale HTTP Protokoll findet hier noch eine Verschlüsselung der Daten statt.

Eine weitere Kommunikation zwischen Kunde und Bank, deren Sicherheit sehr wichtig ist, ist die Übermittlung von Daten bei der Nutzung der EC-Karte. Zwar befinden sich auf der EC-Karte Informationen wie Kontonummer, Bankinstitut etc., aber der PIN muss sicher übermittelt werden. Hierzu befindet sich auf der EC-Karte ein eigenes kleines Cryptosystem, das die eingegebene PIN verschlüsselt und dann an den Zentralcomputer der Bank schickt.

Zwar hörte man in den vergangenen Jahren viel über abgehörte Handytelefonate (auch von wichtigen Personen des öffentlichen Lebens wie Frau Merkel), obwohl auch das Telefonnetz

für Mobiltelefone verschlüsselt ist. Jedoch ist die Verschlüsselung sehr schwach, so dass es zwar für Privatpersonen zu aufwändig, aber für Behörden wie die NSA oder dem BND ohne weiteres möglich ist.

6.2 Grober Unterrichtsplan (exemplarisch)

Unterrichtsszenarien	Kurze Zusammenfassung
Einstieg	Schülerinnen und Schüler durchlaufen die Detektivgeschichte rund um den Pudel Rex und lernen dabei verschiedene kryptographische Verfahren kennen.
Vertiefung	Schülerinnen und Schüler lernen moderne Verfahren kennen und wenden diese praktisch an. Dabei verschlüsseln sie E-Mailnachrichten und Dateien.
Abschluss	Schülerinnen und Schüler sehen den Film zu *„Men in Grey“* und besprechen die Bedeutung von sicherer Kommunikation und Verschlüssellung im Alltag.

6.3 Stundenverlaufsskizzen

Abkürzungen/Legende
AB = Arbeitsblatt/Arbeitsblätter; L = Lehrkraft; MuM = Mitschülerinnen und Mitschüler; SuS = Schülerinnen und Schüler;
UV = Unternehmensvertreterin/Unternehmensvertreter

Detektivgeschichte

Zeit	Phase	Sozialform/ Lehrerimpuls	Inhalt/Unterrichtsgeschehen	Material
Vorbereitung			L sendet den SuS die erste E-Mail der Detektivgeschichte. Hier ist es notwendig, dass die E-Mailadressen vorher vom L gesammelt werden. Sie sollten sich gegebenenfalls informieren, ob nicht bereits ein E-Mailverteiler existiert.	A2.1
10 Min.	Einsteig	Plenum	Begrüßung der SuS; Erklärung des neuen Themenkomplexes; Aufgabenstellung (MindMap und E-Mail) erklären; Flipchart/ Metaplanpapier verteilen Frage: *Wie kann man die Nachricht entschlüsseln? Gibt es einen Hinweis auf die Verschlüsselung?* MindMap: Als einzige Vorgabe wird der Begriff *Kryptologie* in die Mitte geschrieben.	
25 Min.	Erarbeitung	Einzel-/Partner-/Gruppenarbeit[2]	Die SuS bearbeiten die erste Nachricht und Antworten auf die E-Mail.	
10 Min.	Sicherung	Plenum	Besprechung des Vorgehens und Lösung.	

[2] Welche Sozialform hier gewählt wird, liegt vollkommen bei der Lehrkraft, da alle drei möglich sind.

Zeit	Phase	Sozialform/ Lehrerimpuls	Inhalt/Unterrichtsgeschehen	Material
Vorbereitung			L sendet den SuS die zweite E-Mail der Detektivgeschichte.	A2.1
5 Min.	Einsteig	A2.1	Begrüßung der SuS; Erklärung der Aufgabenstellung (MindMap und E-Mail)	
30 Min.	Erarbeitung	Einzel-/Partner-/Gruppenarbeit	Die SuS bearbeiten die zweite Nachricht und Antworten auf die E-Mail.	
10 Min.	Sicherung	Plenum	Besprechung des Vorgehens und Lösung.	

Zeit	Phase	Sozialform/ Lehrerimpuls	Inhalt/Unterrichtsgeschehen	Material
Vorbereitung			L sendet den SuS die dritte E-Mail der Detektivgeschichte.	A2.1, A2.2
5 Min.	Einsteig		Begrüßung der SuS; Erklärung der Aufgabenstellung (MindMap und E-Mail)	
30 Min.	Erarbeitung	Einzel-/Partner-/Gruppenarbeit	Die SuS bearbeiten die dritte Nachricht und Antworten auf die E-Mail.	
10 Min.	Sicherung	A2.1	Besprechung des Vorgehens und Lösung. L sendet den SuS die vierte E-Mail der Detektivgeschichte.	A2.1
Hausaufgabe			Die SuS können ihre MindMap nochmals überarbeiten.	

Zeit	Phase	Sozialform/ Lehrerimpuls	Inhalt/Unterrichtsgeschehen	Material
	Vorbereitung		L sendet den SuS die fünfte E-Mail der Detektivgeschichte.	A2.1, A2.3
5 Min.	Einsteig	Plenum	Begrüßung der SuS; Aufgabenstellung klären (MindMap und E-Mail)	

30 Min.	Erarbeitung	Einzel-/Partner-/Gruppenarbeit	Die SuS bearbeiten die fünfte und sechste Nachricht und Antworten auf die E-Mail. Während der Bearbeitung der fünften E-Mail sendet L den SuS die sechste E-Mail der Detektivgeschichte.	A2.1, A2.4
10 Min.	Sicherung	Plenum	Besprechung des Vorgehens und Lösung. L sendet den SuS die siebte E-Mail der Detektivgeschichte.	A2.1, A2.5
Hausaufgabe			Die SuS senden dem L (Sarah und Max) die fertige MindMap zu.	

Abschluss

Zeit	Phase	Sozialform/ Lehrerimpuls	Inhalt/Unterrichtsgeschehen	Material
30 Min.	Einstieg	Lehrervortrag	L bespricht mit den SuS den bisheriegen Fortschritt und leitet den Abschluss dieses Themas ein. L sollte dabei den SuS die Funktionsweise von Public- und Private-Keys erklären und den Unterschied zu den bisherigen einfachen Verfahren (Caesar, Vigenére …) aufzeigen.	A2.6
30 Min.	Vertiefung II	Einzel-/Partnerarbeit	Die SuS bearbeiten das Arbeitsmaterial V3.8 und verschlüsseln Dateien mittels verschiedener Softwarelösungen.	A2.7
30 Min.	Reflexion	Think-Pair-Share	L zeigt den SuS den Film zu Men in grey; Besprechung verschiedener Fragestellungen zur sicheren Kommunikation etc.	

7 Einbettung in verschiedene Fächer und Themen

Als Einbettung in ein speziellen Unterrichtsfach bietet sich in erster Linie die Informatik oder Technik an. Da gerade die Informatik nicht in allen Bundesländern fester Bestandteil der Schuldbildung ist und einige Schulen kein Unterrichtsfach in Richtung der Informatik anbieten, würde es sich als Alternative anbieten, dieses Modul fächerübergreifend im Rahmen einer Projekt- bzw. Themenwoche einzubinden.

Die folgenden Kompetenzen finden sich entweder in den Bildungsstandards der Kultusministerkonferenz oder in den einzelnen Rahmenlehrplänen der Länder wieder:

Informatik/Technik

Die Schülerinnen und Schüler …

- kennen ausgewählte Beispiele von Algorithmen/Verfahren zum Ver- und Entschlüsseln von Nachrichten sowie zum Knacken eben dieser.
- kennen die Bedeutung von krytographischen Verfahren bzgl. sicherer Kommunikationen sowie die damit verbundene gesellschaftliche aber auch wirtschaftliche Bedeutung.
- reflektieren ihren eigenen Umgang mit sicheren und unsicheren Übertragungswegen und können sich absichern.
- kommunizieren fachgerecht über informatische Sachverhalte.
- veranschaulichen kryptologische Sachverhalte. (Optional)
- implementieren kryptographische Verfahren mittels geeigneten Verfahren. (Ausblick)

Mathematik

Für eine Lehrkraft bedeutet die Einbindung dieses Moduls im Mathematikunterricht wahrscheinlich eher eine Ausrichtung bezüglich der Verfahren, weshalb hier gilt:

Die Schülerinnen und Schüler …

- können geeignete heuristische Hilfsmittel, Strategien und Prinzipien zum Problemlösen auswählen und anwenden.
- können die Plausibilität der Ergebnisse überprüfen sowie das Finden von Lösungsideen und die Lösungswege reflektieren.
- können Überlegungen, Lösungswege bzw. Ergebnisse dokumentieren, verständlich darstellen und präsentieren, auch unter Nutzung geeigneter Medien.

8 Anschlussthemen

Als Anschlussthemen im Zusammenhang mit IT2School bieten sich folgende Module an:

Beispiel: Programmieren

→

oder

Gerade hinsichtlich dem Modul B5 und A3 empfiehlt sich eine mögliche Vertiefung dieses Moduls bei dem die Schülerinnen und Schüler die erlernten Verfahren selbstständig in Form von Programmen in Scratch bzw. Python implementieren. Besonders die aufwändigeren Verfahren zum entschlüsseln von kryptographischen Verfahren bietet sich hier an.

9 Literatur und Links

- Simon Singh. **Codes – Die Kunst der Verschlüsselung**. 2001. Hanser Verlag. ISBN: 3-446-20169-6
- Didaktik der Informatik der Universität Wuppertal. **Spioncamp**. URL: http://ddi.uni-wuppertal.de/material/spioncamp.html
- Informatik Schule. **Kryptologie**. URL: http://www.inf-schule.de/kommunikation/kryptologie
- Informatik im Kontext: **E-Mail (nur) für Dich?** URL: http://www.informatik-im-kontext.de/
- **Morsecode:** http://morsecode.scphillips.com/translator.html

10 Arbeitsmaterialien

Nr.	Titel	Beschreibung
A2.1	Detektivgeschichte	Enthält die E-Mailnachrichten, welche den Schülerinnen und Schülern gesendet werden sollen.
A2.2	Anhang für dritte E-Mail	Bild der zu knackenden fleißnerschen Schablone
A2.3	Anhang für fünfte E-Mail	ZIP-Archiv, das OpenPuff mit Anleitung, schluesselwoerter.png und den Kalender enthält.
A2.4	Anhang für sechste E-Mail	Anleitung zur Verschlüsselung von E-Mails.
A2.5	Anhang für siebte E-Mail	Bild von Pudel Rex.

A2.6	Präsentation zur asynchronen Verschlüsselung	Präsentation kann für den Lehrervortrag genutzt werden.
A2.7	Anleitung zu VeraCrypt	Anleitung zur Dateiverschlüsselung mit dem Programm VeraCrypt.
A2.8 bis A2.12	Zusatzmaterial	Dieses Material kann als Alternative zur Detektivgeschichte verwendet werden.

Legende

Material für Schülerinnen und Schüler

Material für Lehrkräfte sowie Unternehmensvertreterinnen und Unternehmensvertreter

Zusatzmaterial

11 Glossar

Begriff	Erläuterung
Atbash-Verschlüsselung	Ein monoalphabetisches Substitutionsverfahren, bei dem der erste Buchstabe des Alphabetes mit dem letzten, der Zweite mit dem vorletzten usw. ausgetauscht wird: • A wird mit Z verschlüsselt und umgekehrt • B wird mit Y verschlüsselt und umgekehrt • Usw.
Caesar-Verschlüsselung	Ein monoalphabetisches Substitutionsverfahren, bei dem das Ursprungsalphabet um einen festen Wert verschoben wird. Bei einer Verschiebung von 3 bedeutet dies: • A wird mit D verschlüsselt • B wird mit E verschlüsselt • Usw.
Chiffre	Bezeichnet einen verschlüsselten Text.
Chiffrieren	Bezeichnet das Verschlüsseln eines Klartextes.
Enigma	Bie der Enigma handelt es sich um eine sogenannte Rotor-Schlüsselmaschine. Mittels mehrerer Rotoren erfolgt die Generierung vieler Geheimalphabete, welche zur elektronischen Verschlüsselung von Nachrichten im zweiten Weltkrieg von den Deutschen genutzt wurde. Geknackt wurde die Verschlüsselung der Enigma von Alan Turing.
Geheimalphabet	Ein neues permutiertes Alphabet, welches auf Grundlage des Urpsrungsalphabetes des Klartextes durch Verschiebung oder

	Austausch von Buchstaben entsteht.
Hashen	Bezeichnet die Anwendung einer Hash-Funktion zur Generierung eines Hash-Wertes.
Hash-Funktion	Generiert aus einem Wert, welcher aus Zeichen, Zahlen, Dateien etc. bestehen kann, einen neuen Hash-Wert, welcher keine Zurückführung auf den eigentlichen Wert ermöglicht.
Hash-Wert	Ein mittels einer Hash-Funktion generierter Wert, welcher aus Zeichen und Zahlen bestehen kann.
Häufigkeitsanalyse	Ein Verfahren, dass beim Knacken von Entschlüsselungen verwendet wird und gerade bei einfachen monoalphabetischen Verschlüsselungen großen Erfolg verspricht.
Klartext	Ein unverschlüsselter Text.
Kryptoanalyse	Der Teil der Kryptologie, welcher sich mit der Entschlüsselung und Sicherheit befasst.
Kryptographie	Der Teil der Kryptologie, welcher sich mit der Verschlüsselung von Informationen befasst.
Kryptologie	Die Wissenschaft, welche sich mit der Sicherheit von Informationen befasst.
Monoalphabetisches Substitution	Bei Verfahren diesen Typs erfolgt die Substitution mittels eines Geheimalphabetes. Beispiele hierfür sind die Atbash- oder Caesar-Verschlüsselung.
Polyalphabetisches Substitution	Bei Verfahren diesen Typs erfolgt die Substitution mittels mehrerer Geheimalphabete. Beispiel hierfür ist die Vigenère-Verschlüsselung.
Polybius-Verschlüsselung	Ein monoalphabetisches Substitutionsverfahren, bei dem Buchstaben eines Alphabetes in einer Matrix angeordnet werden und anschließend durch deren Koordinaten ersetzt werden.
Semagramme	Dies ist eine Bezeichnung aus der Steganographie und bezeichnet einen unverfänglichen Text, Bild etc., in dem sich eine verstecke Geheimnachricht befindet.
Skytale-Verschlüsselung	Ein Transpositionsverfahren, bei dem ein Papier- oder Lederstreifen um einen Stab mit bestimmten Durchmesser (der sogenannte Skytale) gewickelt wird und auf welchem die Nachricht geschrieben wird.
Steganographie	Der Teil der Kryptologie, welcher sich mit der Verschleierung von Informationen befasst.
Substitution	Fasst alle Verfahren zusammen, bei dem Buchstaben, Symbole oder Wörter eines Klartextes durch andere ersetzt werden.
Transposition	Fasst alle Verfahren zusammen, bei dem Buchstaben, Symbole oder Wörter nicht ersetzt, sondern verschoben werden.
Vigenère-Verschlüsselung	Ein polyalphabetisches Substitutionsverfahren, welches der Caesar-Verschlüsselung ähnelt, aber bei dem mehrere durch ein

	Schlüsselwort bestimmte Geheimalphabete verwendet werden.

Detektivgeschichte

Nachfolgend finden Sie alle E-Mails zur Durchführung der Detektivgeschichte. Diese können Sie einfach in ihr E-Mail-Programm kopieren, um Sie ihren Schülerinnen und Schülern zuzusenden. Zusätzlich finden Sie Vorlagen für die folgenden sieben E-Mails als .eml-Format im digitalen Archiv, die sich mit gängigen E-Mail-Programmen öffnen und so einfach an Ihre Schülerinnen und Schüler versenden lassen.

Erste E-Mail

Hi,

cool, dass du unserem Detektivklub beigetreten bist. Wir (Sarah und Max) sind die Hauptdetektive unseres Klubs. Da es aber viel zu tun gibt, freuen wir uns sehr über deine Unterstützung und hoffen, dass wir zusammen viele Fälle lösen können!

Apropos lösen können … wir haben da heute eine seltsame Nachricht per E-Mail zugesandt bekommen. Auch wenn Max meinte, dass das nur Spam ist, könnte sich mehr dahinter verbergen. Kannst du herausfinden, was dahintersteckt? Unten findest du den Betreff und den Inhalt der E-Mail.

Solltest du es herausgefunden haben, dann antworte auf diese E-Mail und schicke uns den Inhalt der obigen Nachricht. Außerdem ist es wichtig für unseren Klub, dass neue Sachen dokumentiert werden. Erstelle also bitte eine MindMap zum Thema Kryptologie. Viel Erfolg!

Liebe Grüße
Sarah und Max

Betreff: Apzia ivxc Gdifn

Cvggj Yzozfodqz,

dxc cvwz zdizi bzczdhzi Vpaomvb aüm zpxc. Yjxc qjmczm hpnn dxc rdnnzi, jw dcm nj bpo nzdy, rdz dcm wzcvpkozo piy ydznz Qzmnxcgpznnzgpib fivxfzi fjziio.

Gdzwz Bmpznnz
yzm Piwzfviioz

Unverschlüsselte Nachricht – Nicht an die Schülerinnen und Schüler herausgeben!!!

Betreff: Fuenf nach Links

Hallo Detektive,

ich habe einen geheimen Auftrag für euch. Doch vorher muss ich wissen, ob ihr so gut seid, wie ihr behauptet und diese Verschluesselung knacken könnt.

Liebe Gruesse
der Unbekannte

Zweite E-Mail

Hi,

super Einfall von dir. Wir hätten nicht gedacht, dass es sich um eine Verschlüsselung handelt. Du bist wirklich eine Bereicherung für unseren Klub! Wir haben den Unbekannten kontaktiert und eine neue E-Mail von ihm erhalten, die wir dir unten mal weitergeleitet haben.

Es scheint wirklich dringend zu sein, du solltest versuchen, die Verschlüsselung zu knacken. Dieses Mal scheinen die Buchstaben durch Zahlen ersetzt worden zu sein. Es handelt sich also wieder um eine Substitution. Sobald du die Nachricht entschlüsselt hast, schick sie uns zu. Viel Erfolg!

Liebe Grüße
Sarah und Max

PS: Denke bitte an deine MindMap. Der Begriff Substitution scheint wichtig zu sein und sollte in der MindMap auftauchen.

Betreff: Eine Entführung

Gut gemacht Detektive!

Es freut mich, dass ihr doch so gut seid, wie ihr behauptet. Ich habe einen sehr dringenden Entführungsfall, um den ihr euch kümmern müsst. Bevor ihr fragt, ja ich bin mir sicher, dass es sich um eine Entführung handelt!

Den einzigen Hinweis, den ich bezüglich der Täter habe, ist folgender Zettel (siehe Anhang), den ich gefunden habe. Er scheint eine verschlüsselte Botschaft zu enthalten (daher auch der Test mit der Caesar-Verschlüsselung).

Bitte helft mir, es ist dringend!

Anhang (Nachricht verschlüsselt mit Polybius 5*5 Matrix und i=j)

14 11 43 55 24 15 31 12 15 21 24 33 14 15 44 43 24 13 23 24 32 32 15 42 51 34 33 11 13 23 44 12 24 43 55 15 23 33 45 23 42 14 42 11 45 43 43 15 33 51 34 42 14 15 32 23 11 45 43 ...
43 13 23 31 11 22 15 14 11 33 33 55 45 45 33 14 43 13 23 33 11 35 35 14 24 15 43 15 33 42 15 53 !
33 24 32 32 11 33 43 13 23 31 24 15 15 33 14 14 15 33 12 45 43 24 33 42 24 13 23 44 45 33 22 24 33 33 15 33 43 44 11 14 44 .
14 11 33 33 33 24 32 32 14 15 33 13 34 32 35 45 44 15 42 23 24 33 44 15 33 31 24 33 25 43 24 32 24 33 44 15 42 33 15 44 13 11 21 15 … 14 45 21 24 33 14 15 43 44 14 34 42 44 52 15 24 44 15 42 15 11 33 52 15 24 43 45 33 22 15 33 31 34 15 43 13 23 15 14 11 33 11 13 23 14 24 15 11 33 52 15 24 43 45 33 22 15 33 !

Unverschlüsselte Nachricht

Das Ziel befindet sich immer von acht bis zehn Uhr draussen vor dem Haus …
Schlage dann zu und schnapp diesen Rex!
Nimm anschließend den Bus in Richtung Innenstadt.
Dann nimm den Computer hinten links im Internetcafe … du findest dort weitere Anweisungen.
Loesche danach die Anweisungen!

Dritte E-Mail

Hi,

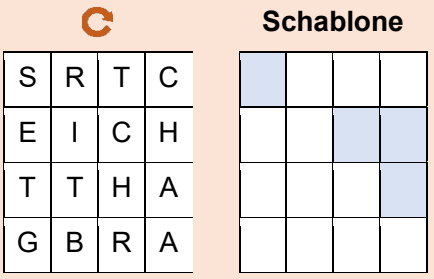
wunderbare Arbeit von dir! Ich (Ingo, ebenfalls ein neues Mitglied) kümmere mich nun um die Kommunikation mit dem Unbekannten, Sarah und Max untersuchen die Spuren (Bus und Internetcafé). Wer wohl dieser Rex ist? Sobald Sarah und Max etwas Neues wissen, werde ich dich informieren.

Der Unbekannte hat uns übrigens noch einen weiteren Zettel (siehe Anhang) zukommen lassen, den er gefunden hat. Auf der Rückseite des Zettels steht „Passwort“ geschrieben. Das ist bestimmt wichtig! Es scheint, als wenn es dieses Mal keine Substitution ist. Was für eine Art von Verschlüsselung ist es diesmal? Kannst du mal schauen, ob du auf das Passwort kommst und es mir dann zuschicken? Es könnte sein, dass es Sarah und Max im Internetcafé brauchen.

Liebe Grüße
Ingo

PS: Ich bin froh, dass du alles in der MindMap festhältst, es werden langsam viele Informationen. Diese neue Art von Verschlüsselung müsste dort auch eingefügt werden.

Anhang (fleißnersche Schablone)



Lösung – Nicht an die Schülerinnen und Schüler herausgeben!!!

SCHACHBRETTARTIG

Vierte E-Mail

Hi,

deine E-Mail kam genau zum richtigen Zeitpunkt!

Wir (Sarah und Max) konnten uns mit diesem Passwort als Benutzer am Computer anmelden. Nun versucht Lisa (auch ein Mitglied unseres Klubs), die privaten Dateien des Accounts auszuwerten.

Für dich heißt es momentan also Pause machen. Hast du dir auch verdient ;-). Sobald wir mit der Auswertung der Dateien fertig sind, werden wir dich informieren. Wir freuen uns schon auf deine MindMap! Bitte nutze die Zeit um sie vielleicht noch zu überarbeiten.

Übrigens wissen wir nun wer Rex ist! Das ist der Pudel des Unbekannten. Der Besitzer des Internetcafés hat zwar den Hund bemerkt, aber nicht den Entführer. Sehr schade …

Liebe Grüße
Sarah und Max

Fünfte E-Mail

Hi,

die Auswertung der Dateien war sehr aufschlussreich. Wir haben einen Kalender gefunden, wobei die Einträge wieder verschlüsselt sind. Diesmal haben wir direkt versucht, die Verschlüsselung mit Caesar zu knacken, aber das hat nicht funktioniert. Das heißt, dass du mal wieder dran bist :-).

Außerdem haben wir noch eine Datei *schluesselwoerter.png* gefunden. Wir vermuten, dass die Entführer in diesem Bild eine weitere Datei versteckt haben. Zumindest meinte Lisa, dass das möglich ist. Sie hat aber gerade keine Zeit dafür. Daher brauchen wir auch hier deine Hilfe. Sie gab uns den Tipp das Programm OpenPuff zu verwenden (Anleitung ist angehängt). Vielleicht kannst du das notwendige Passwort aus dem Bild entnehmen.

Warte übrigens mit deiner Antwort ab. Lisa versucht gerade unsere E-Mails abzusichern. Du bekommst später noch eine weitere E-Mail.

Viel Erfolg!

Liebe Grüße
Sarah und Max

PS: Wie steht es um die MindMap? Füge auch die neue Art von Verfahren hinzu. Es sollte auch klar werden, wie sie sich zwei Verfahren der gleichen Art voneinander unterscheiden können.

Lösung – Nicht an die Schülerinnen und Schüler herausgeben!!!

Codewort für openpuff lautet FEHLERFREI (wenn man sich schluesselwoerter.png anschaut kommt man recht schnell drauf). Damit können aus dem Bild die folgenden Codewörter extrahiert werden:

SPORT
FREUNDE
AUFTRAG
NOTIZEN

Mit diesen Codewörtern lassen sich die Kalendereinträge wie folgt mittels des Vigenere-Verfahrens entschlüsseln (Tipp: https://einklich.net/etc/vigenere.htm ist eine gute Hilfe, sobald man das Vigenere-Verfahren bereits verstanden hat und Zeit sparen möchte):

```
02.09. 18:00   Xxhexkhgknvxc                  Fitnessstudio                 (Sport)
05.09. 19:00   Ryc rbnofjg                    Rex abholen                   (Auftrag)
08.09. 21:00   Ryc zm Cogxj hec Erry ugzvbkn  Rex im Cubes bei Lars abgeben (Auftrag)
09.09. 18:00   Xxhexkhgknvxc                  Fitnessstudio                 (Sport)
13.09. 16:00   Tywfzn byn uex Vfgb            Termin bei der Bank           (Auftrag)
16.09. 18:00   Xxhexkhgknvxc                  Fitnessstudio                 (Sport)
17.09. 20:00   Lvfoevxfxjyvhv msh Mes         Geburstagfeier von Jan        (Freunde)
23.09. 18:00   Xxhexkhgknvxc                  Fitnessstudio                 (Sport)
27.09. 16:00   Yiizshr dmn Oezie              Treffen mit Laura             (Freunde)
30.09. 18:00   Xxhexkhgknvxc                  Fitnessstudio                 (Sport)

Notizen:       Uigldjhghxz onhtxv!            Hundefutter kaufen.           (Notizen)
               Piumr -> Uitqtnfmmmwgeolad 3   Cubes -> Baumgartenstrasse 3  (Notizen)

Geburtstage:   17. Orr                        Jan                           (Freunde)
               29. Mrrhrv                     Hannes                        (Freunde)
```

Sechste E-Mail

Hi,

es ist besser, wenn wir ab sofort unsere E-Mails verschlüsseln. Wir verwenden dazu nun PGP. Habe dir eine Anleitung mit Erklärung sowie unseren Public-Key angehängt. Solltest du uns schreiben, dann verschlüssele deine E-Mail mit diesem Schlüssel.

Konntest du den Kalender entschlüsseln? Wenn ja, dann schick uns bitte den entschlüsselten Kalender. Sarah und Max koordinieren das weitere Vorgehen.

Liebe Grüße
Lisa

Siebte E-Mail

Hi,

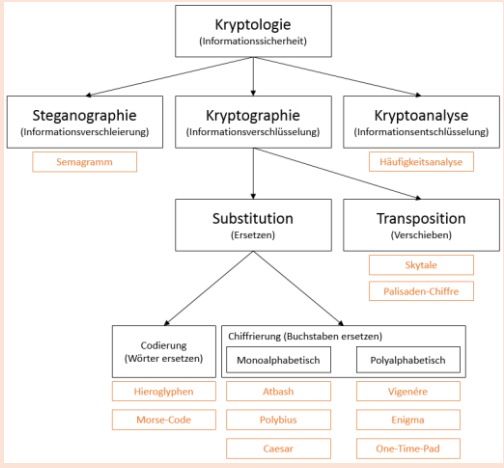
wir konnten die Übergabe von Rex mit Hilfe der Polizei vereiteln! Die Entführer haben Rex entführt, weil dieser schon mehrere Schönheitswettbewerbe gewonnen hat. Nun befindet sich Rex aber wieder bei seinem Herrchen (unserem Biolehrer Herrn Meyer). Wer hätte gedacht, dass Herr Meyer der Unbekannte ist…

Das war sehr gute Arbeit von dir! Hier übrigens noch ein Bild vom nun wieder glücklichen Rex.

Jetzt bräuchten wir nur noch deine MindMap um den Fall für die Polizei auch vollständig dokumentieren zu können. Danke dafür!

Liebe Grüße
Sarah und Max

Mögliche Mind-Map (siehe Modulbeschreibung)



E-Mails verschlüsseln

Die folgende Anleitung zeigt dir, wie du deine E-Mails verschlüsseln kannst. Hierfür brauchst du natürlich eine E-Mailadresse. Sollte es der Fall sein, dass du bisher keine hast, oder das sicherhaltshalber noch nicht mit deiner eigenen E-Mailadresse testen möchtest, kannst du eine von deiner Lehrerin bzw. deinem Lehrer bereitgestellte E-Mailadresse benutzen.

Schritt 1 – Installation von Thunderbird

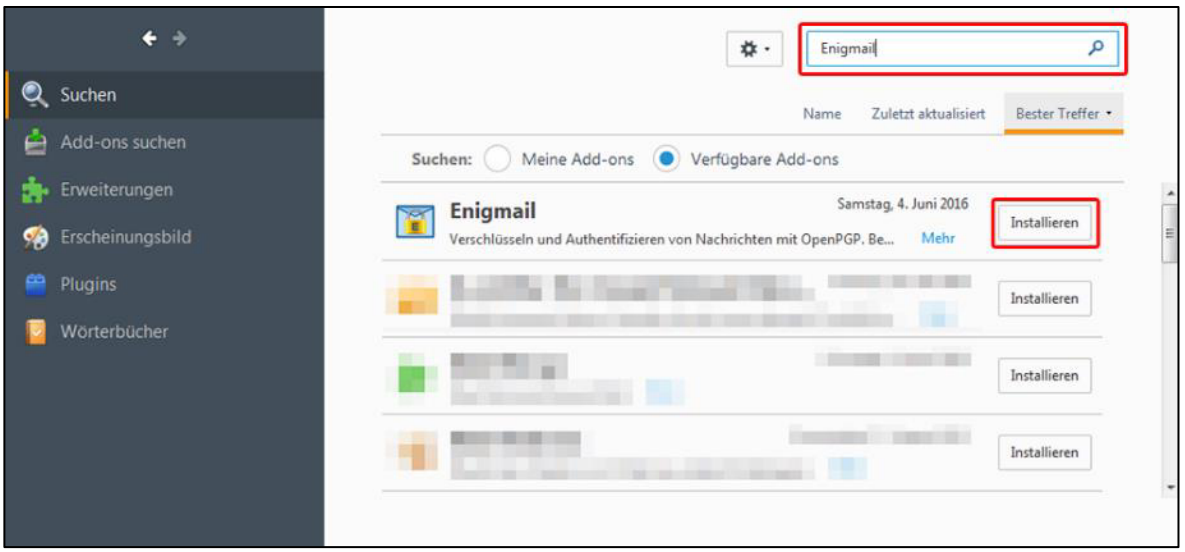
Als E-Mailprogramm verwenden wir Thunderbird. Sollte das Programm noch nicht auf dem Computer installiert sein, dann findest du unter folgender URL die Installationsdatei:

https://www.mozilla.org/de/thunderbird/

Anschließend solltest du das Programm installieren und einen E-Mailaccount einrichten.

Schritt 2 – Installation von Enigmail

Standardmäßig bietet Thunderbird nicht die Möglichkeit E-Mails zu verschlüsseln. Daher benötigen wir das Add-on *Enigmail*. Klicke dazu in der Menüleiste auf den Reiter *Extras* und wähle *Add-ons*. (Sollte die Menüleiste nicht sichtbar sein, musst du die *ALT*-Taste drücken.) Anschließend gibst du in das Suchfeld *Enigmail* ein und kannst das Add-on *installieren*.



Schritt 3 – GnuPG installieren

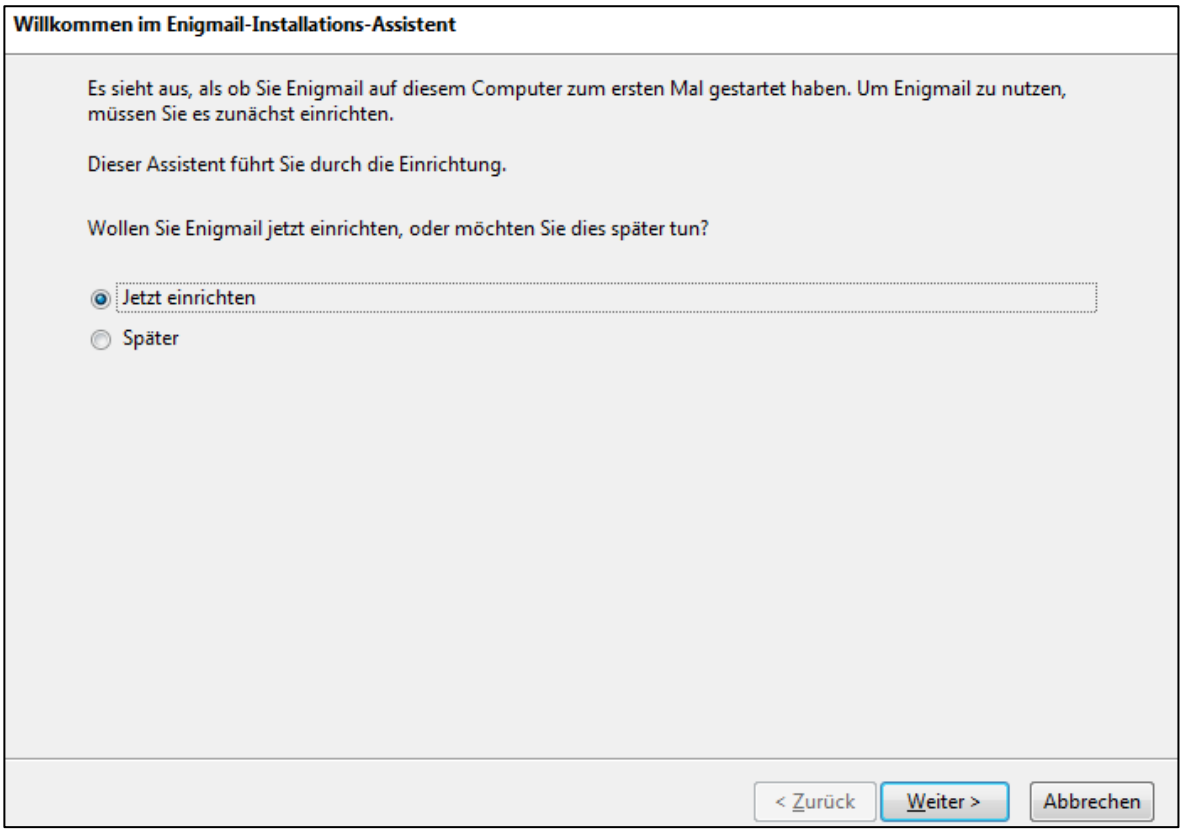
Nach dem das Add-on installiert wurde, kannst du Thunderbird erst einmal schließen (es sollte ein Neustart des Programms notwendig sein). Anschließend benötigen wir noch PGP bzw. die Implementierung GnuPG. Auf der offiziellen Webseite zu GnuPG solltest du ein entsprechendes Programm samt Download für dein Betriebssystem finden (ganz unten auf der Seite unter *GnuPG binasy releases*):

https://www.gnupg.org/download/index.html

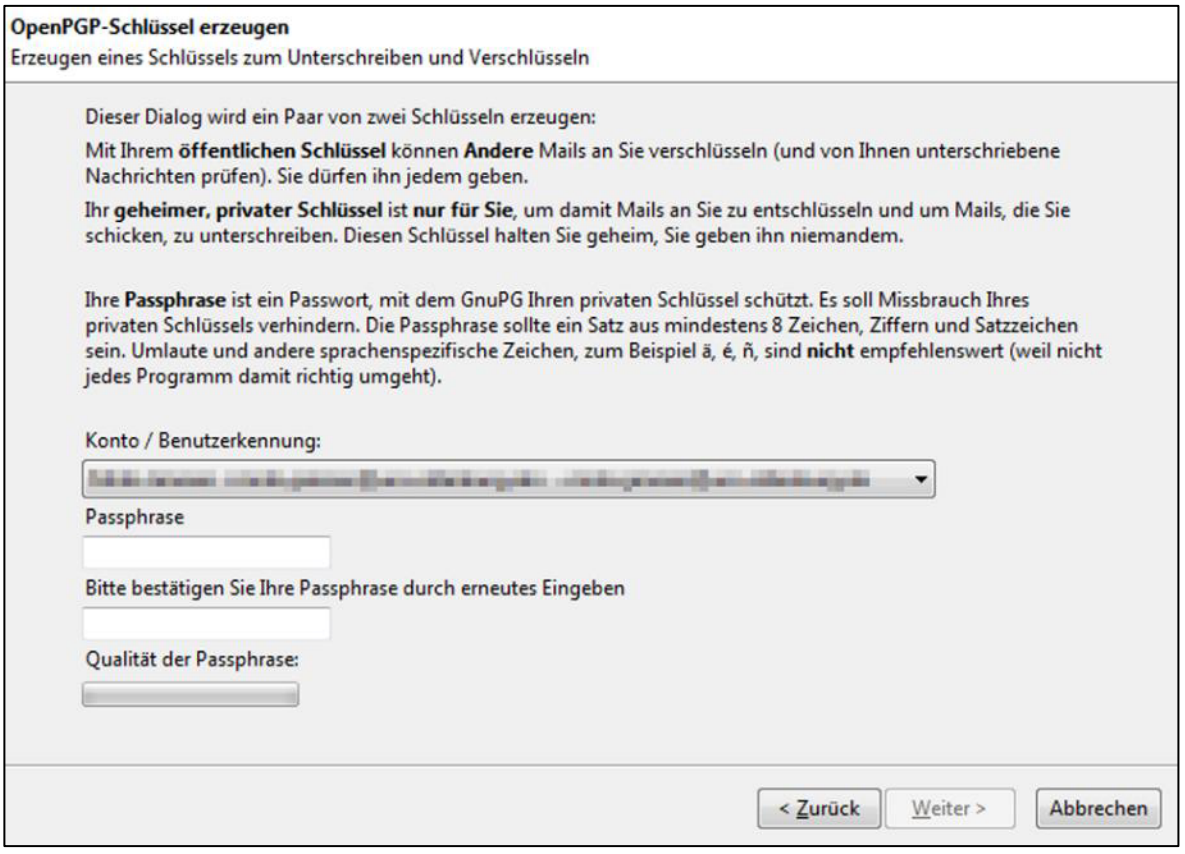
Für Windows kannst du auf Gpg4win klicken und die aktuellste Version herunterladen. Anschließend musst du das Programm noch installieren.

Schritt 3 – Enigmail einrichten

Nach der Installation des Add-ons ist es notwendig, dass du Thunderbird neu startest. Nach dem Neustart öffnet sich ein Fenster mit dem Einrichtungs-Assistenten von Enigmail. Sollte das Fenster nicht erscheinen, so kannst du es unter dem Menüpunkt *Enigmail* > *Einrichtungs-Assistent* aufrufen. Folge anschließend den folgenden Anweisungen.

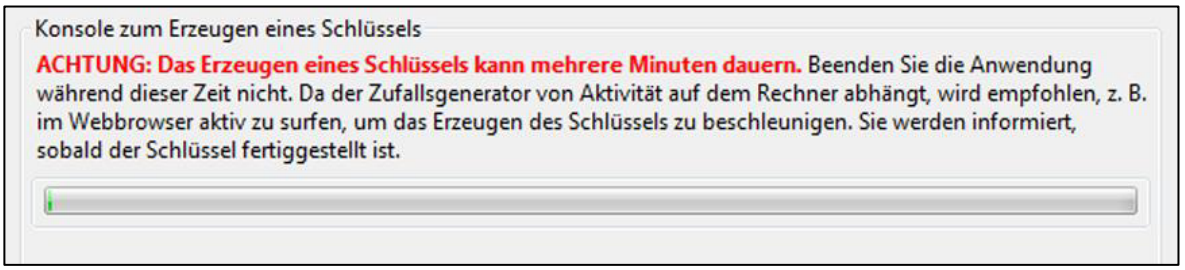


Wähle *Jetzt einrichten* aus und klicke auf *Weiter* >. Anschließend kannst du auswählen, dass du die *Standard-Konfiguration bevorzugst* und dann auf *Weiter* > klicken. Sollte dir im nächsten Schritt angezeigt werden, dass GnuPG (eine Umsetzung von PGP) benötigt, dann wähle den entsprechenden Pfad zu GnuPG aus und klicke auf *Weiter* >. Nun solltest du die Aufforderung erhalten, einen OpenPGP-Schlüssel zu erzeugen.



Um ein Schlüsselpaar zu erzeugen benötigt der Assistent eine Passphrase (ein Passwort). Achte darauf, dass es möglichst sicher ist, d. h. dass die Qualitätsleiste möglichst voll ist.

Sobald du auf Weiter > geklickt hast, sollte das Schlüsselpaar generiert werden. Dies kann einige Zeit benötigen.

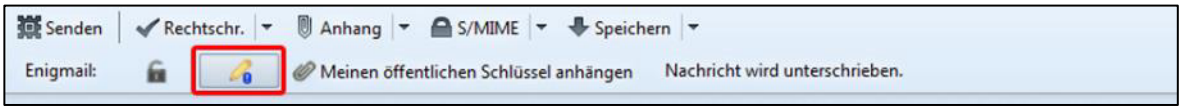


Speichere nun sicherheitshalber noch das Widerrufszertifikat ab. Dabei solltest du darauf achten, dass du es jetzt oder später an einen sicheren Ort ablegst. Das Widerrufszertifikat dient dazu, das soeben generierte Schlüsselpaar, dass nun mit deiner E-Mailadresse verknüpft ist, zu widerrufen. Mit einem Klick auf Weiter > ist die Einrichtung für deinen E-Mailaccount abgeschlossen.

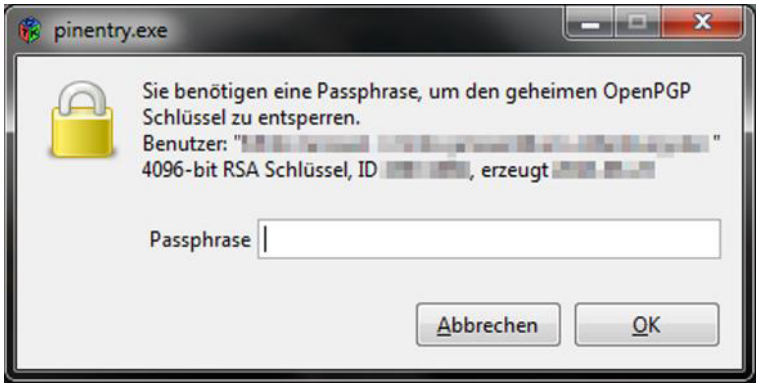
Schritt 4 – Eine verschlüsselte E-Mail verschicken

Sobald du nun in Thunderbird eine E-Mail verschicken willst, hast du die Möglichkeit diese zu unterschreiben und/oder zu verschlüsseln.

Beachte, dass du zum Verschlüsseln einer Nachricht den öffentlichen Schlüssel des Empfänger benötigst. Solltest du diesen nicht besitzten, wirst du vor dem Versenden gefragt, welchen Schlüssel du verwenden willst. Es empfiehlt sich also, nach dem Erzeugen eines Schlüsselpaares den eigenen öffentlichen Schlüsseln mit deinen Bekannten und Freunden auszutauschen. Beim unterschreiben einer E-Mail wird der öffentliche Schlüssel automatisch beigefügt, außerdem weiß der Empfänger so, dass du der Absender bist.



Versendest du eine verschlüsselte oder unterschriebene Nachricht, dann wirst du immer nach der dazugehörigen Passphrase gefragt.



Wissensfabrik
Mehr Wissen. Mehr Können. Mehr Zukunft.

IT2SCHOOL – GEMEINSAM IT ENTDECKEN

MODERNE KRYPTOLOGIE

VORWORT

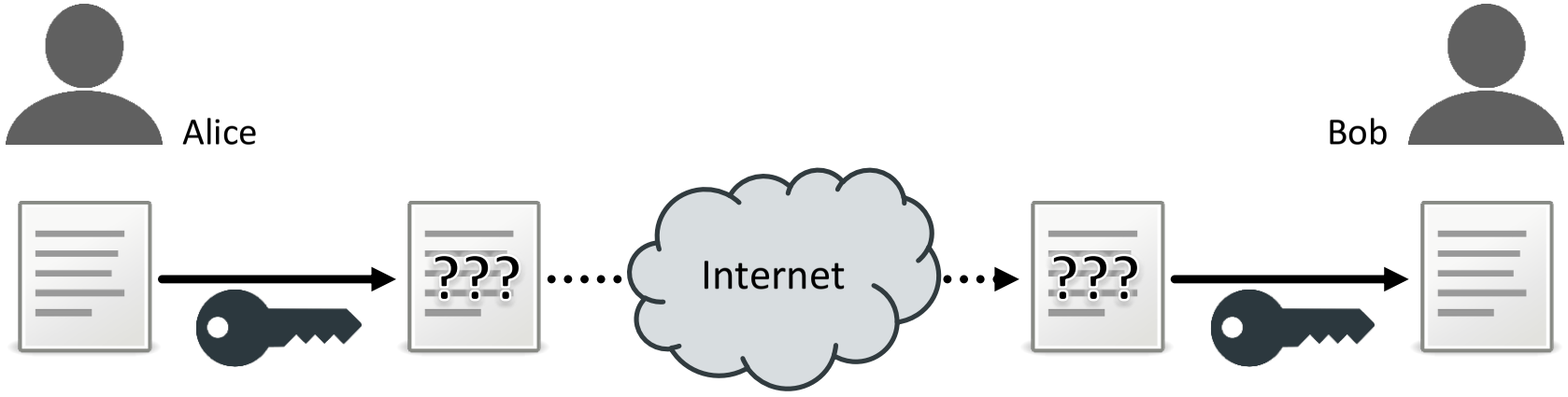
Die Mathematik ermöglicht es die uns bekannte Kryptologie zu modernisieren und komplexere Verfahren zu entwickeln!

Wie dies genauer funktioniert wird euch auf den folgenden Folien gezeigt. Wichtige Grundlagen dafür sind:

- symmetrische und asymmetrische Verschlüsselung
- Public- und Private-Keys
- RSA
- PGP

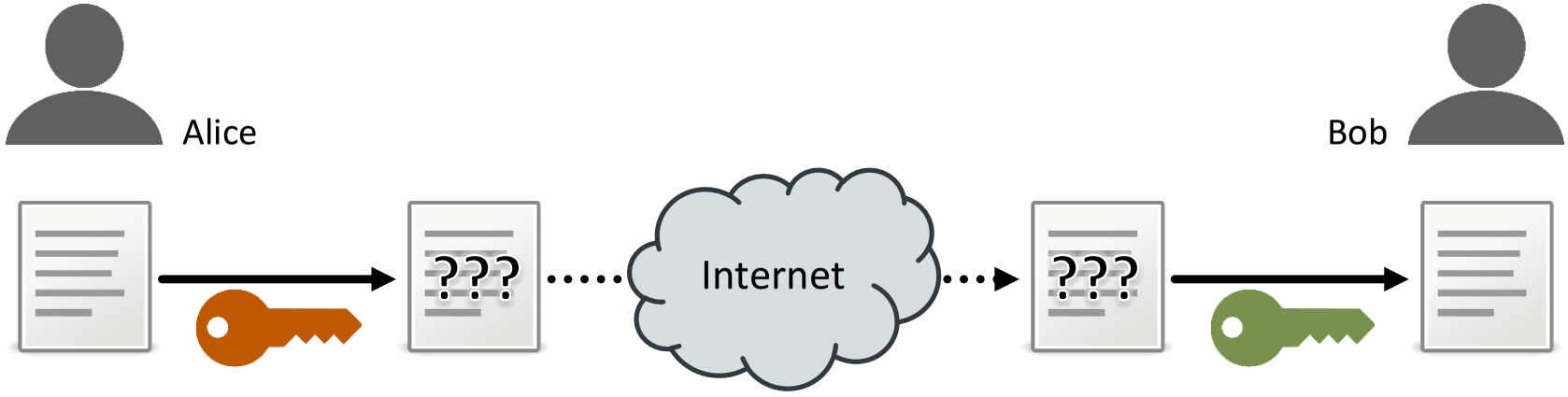
SYMMETRISCHE VERSCHLÜSSELUNG

Alice schickt Bob eine verschlüsselte Nachricht über das Internet.
Zum Ver- und Entschlüsselt wird der selbe Schlüssel bzw. das selbe Verfahren verwendet.



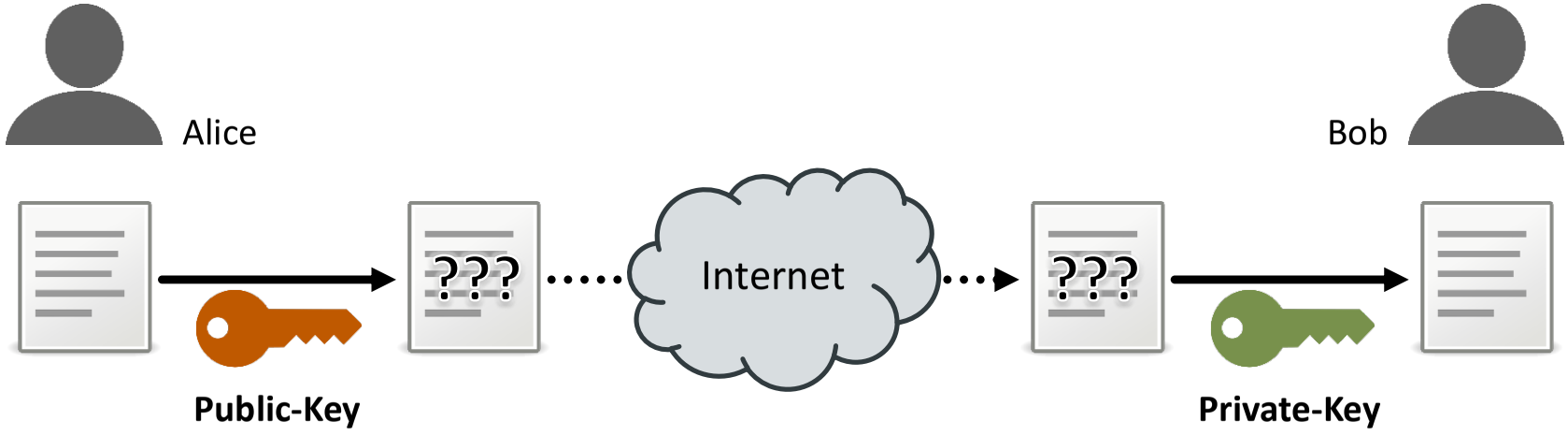
ASYMMETRISCHE VERSCHLÜSSELUNG

Alice schickt Bob eine verschlüsselte Nachricht über das Internet.
Zum Ver- und Entschlüsselt wird nicht der selbe Schlüssel bzw. das selbe Verfahren verwendet.



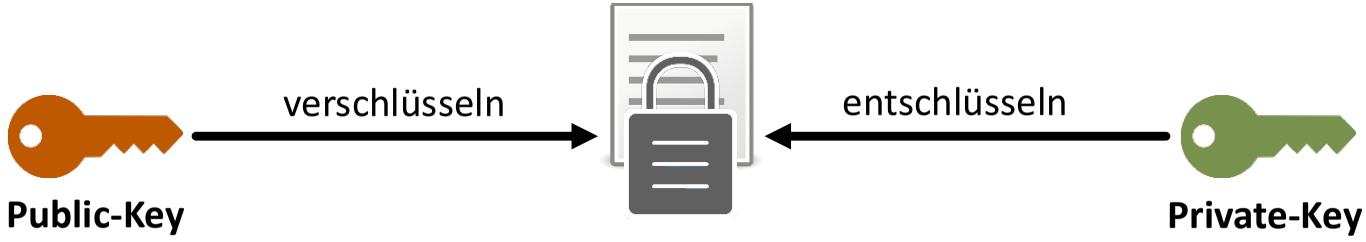
PUBLIC- UND PRIVAT-KEY

Bei der asymmetrischen Verschlüsselung wird ein Schlüssel bekannt gegeben, um die Nachrichten an eine Person zu verschlüsseln und einer wird geheim gehalten, um die verschlüsselten Nachrichten zu entschlüsseln.



PUBLIC- UND PRIVAT-KEY

Wichtig ist, dass der Public- und Private-Key ein Schlüsselpaar sind und immer zusammen gehören bzw. zusammen erstellt werden. Bildlich gesprochen, sind beide für das gleiche Sicherheitsschloss zuständig, nur einer dient zum zuschließen und der andere zum öffnen.



UND WAS HAT DAS MIT DEN BISHERIGEN VERFAHREN ZU TUN?

- Bisher hatten wir im Unterricht nur symmetrische Verfahren, meist auch nur mit Substitution
  - Zum Ver- und Entschlüsseln (bei Caesar, Vigenére etc.) wurde immer das gleiche Schlüsselwort oder Verfahren verwendet
  - Buchstaben werden nur durch andere Buchstaben ausgetauscht
- Bisher noch keine besondere Mathematik oder Logik in den Verfahren
  - Erlaubt uns Buchstaben zu codieren und dann zu verschlüsseln
  - Erlaubt uns Schlüsselpaare zu erzeugen
  - Ein Beispiel dafür ist RSA

RSA

- Benannt ist das Verfahren nach seinen drei Entwicklern:
  - Rivest
  - Shamir
  - Adleman
- Es gibt mehrere Phasen des Verfahrens:
  - Schlüsselpaar erzeugen
  - Nachricht verschlüsseln
  - Nachricht entschlüsseln

RSA – SCHLÜSSELPAAR ERZEUGEN

- Wir brauchen zwei sehr große Primzahlen p und q
- Es wird das Produkt $pq = F$ berechnet
  - Wichtig ist, dass man anhand des Produkt nicht so leicht erkennen kann, welche Primzahlen verwendet wurden! (Wichtig für die Sicherheit)
- Mit mathematischen Hilfsmitteln werden nun die Zahlen e und d ermittelt
  - (F, e) bilden den Public-Key
  - (F, d)bilden den Private-Key

RSA – NACHRICHT VERSCHLÜSSELN

- Die Nachricht wird so codiert, dass sie aus Zahlen besteht
  - Die Codierung kann z. B. mit dem ASCII Code erfolgen
  - Wir bezeichnen die codierte Nachricht als N
- Zum Verschlüsseln brauchen wir den Public-Key
  - Die Verschlüsselte Nachricht M errechnet sich durch

$$M \equiv N^e \pmod{F}$$

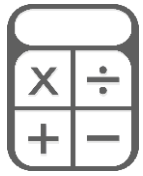
RSA – NACHRICHT ENTSCHLÜSSELN

- Zum Entschlüsseln brauchen wir den Private-Key und die verschlüsselte Nachricht M
  - Die codierte Nachricht N errechnet sich durch

$$N \equiv M^d \pmod{F}$$

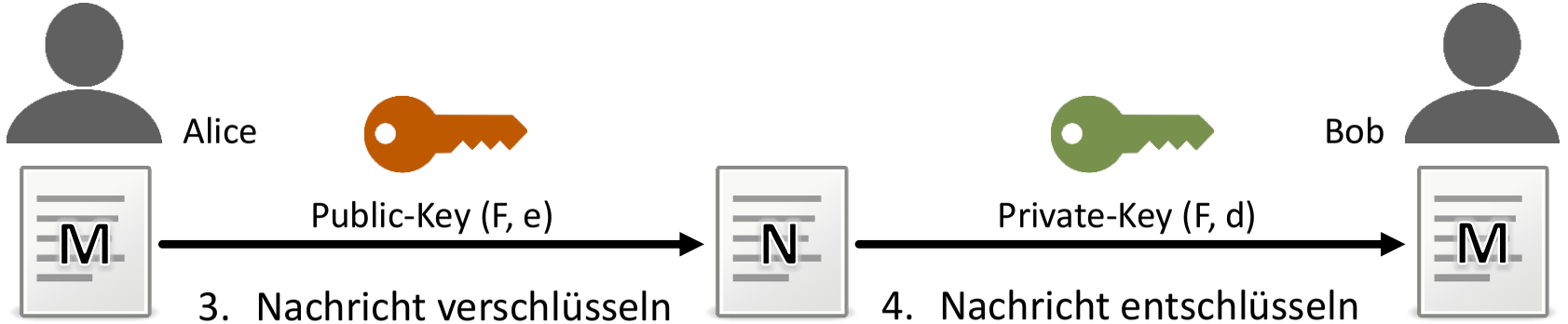
- Die Nachricht N kann nun so codiert werden, dass die ursprüngliche Nachricht lesbar ist
  - Wie die Nachricht codiert wurde, kann sowohl Sender als Empfänger bekannt sein

RSA – SCHAUBILD



1. Große Primzahlen p und q wählen
2. Berechnung von F, e und d

Wichtig ist hier natürlich, dass Bob seinen Public-Key für Alice bereitstellt, damit sie für ihm auch eine Nachricht verschlüsseln kann.



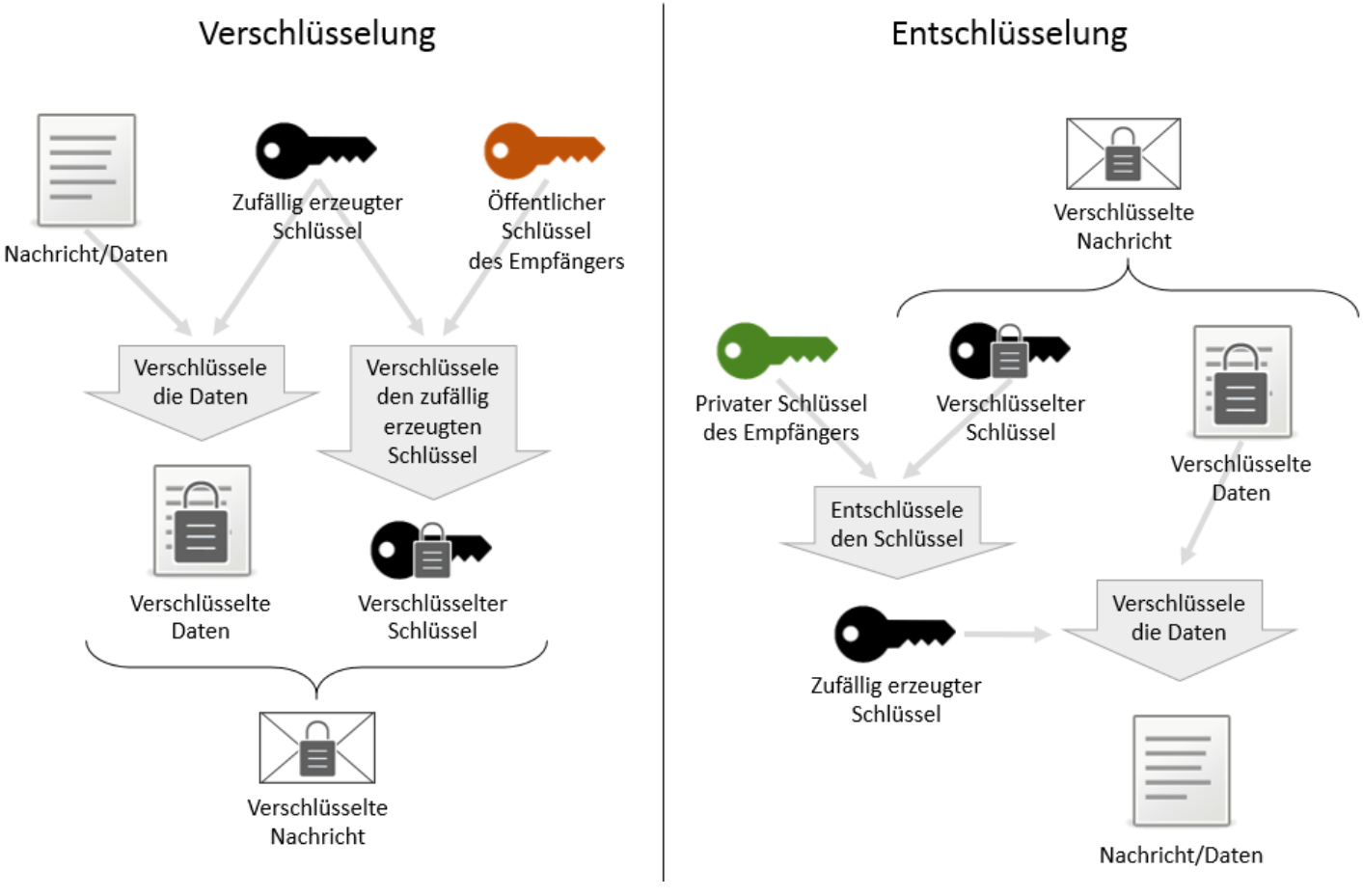
3. Nachricht verschlüsseln
$M \equiv N^e \pmod{F}$

4. Nachricht entschlüsseln
$\mathrm{N} \equiv M^{\mathrm{d}} \pmod{F}$

PGP

- PGP steht für Pretty Good Privacy
- Programm zum Verschlüsseln und Unterschreiben von Daten
- Verwendet hybrides Verfahren aus symmetrischer und asymmetrischer Verschlüsselung
- Verwendete in der ersten Version RSA zum Verschlüsseln (später Elgamal)
- Häufig verwendet zur Verschlüsselung von E-Mails

PGP – SCHAUBILD



Wissensfabrik
Mehr Wissen. Mehr Können. Mehr Zukunft.

Dateien verschlüsseln

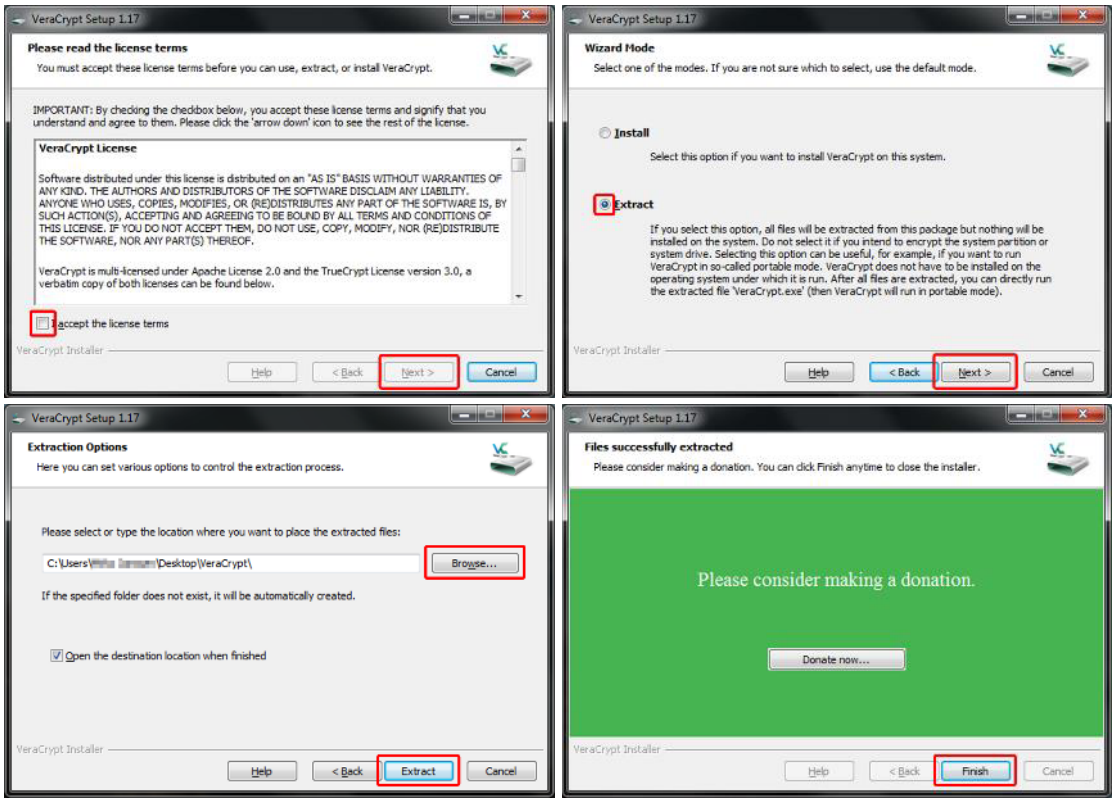
Zum Verschlüsseln von Dateien gibt es mehrere Programme. In dieser Anleitung verwenden wir die kostenlose, opensource Software VeryCrypt. Mit diesem Programm haben wir die Möglichkeit verschlüsselte Kontainer zu erstellen und einzubinden. Dies bedeutet, dass sich auf der Festplatte ein bestimmter Bereich mit verschlüsselten Daten befindet, der nur über diese Software und dem dazugehörigen Schlüssel/Passwort zugänglich gemacht werden kann.

Schritt 1 – Installation

VeryCrypt bietet die Möglichkeit, dass man das Programm auf dem Computer installiert oder aber eine portable Version entpackt. Zum Testen (und eigentlich auch zum Benutzen) reicht die portable Version aus, weshalb wir hier diese Variante benutzen wollen. Solltest du in Zukunft das Programm häufiger nutzen, kannst du es natürlich auch installieren.

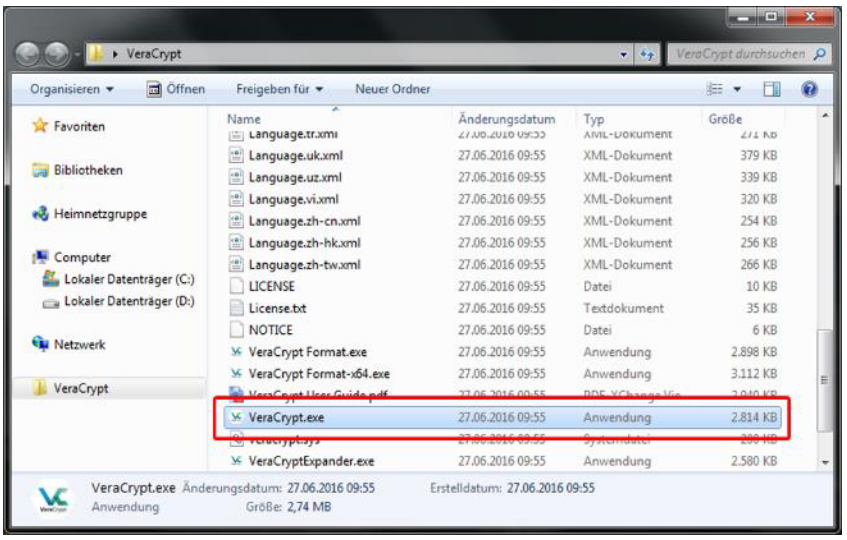
Starte die Installationsdatei und akzeptiere die Lizenzbedingungen. Klicke anschließend auf *Next* > und wähle *Extract* für die portable Variante aus. Klicke wieder auf *Next* >, wähle das Zielverzeichnis aus und klicke anschließend auf *Extract*. Nachdem das Extrahieren beendet ist, kannst du die „Installation“ mittels *Finish* beenden.

Hinweis: Im letzten Schritt wird lediglich um eine Spende (Donation) gebeten. Diese ist zur Nutzung des Programms nicht notwendig.

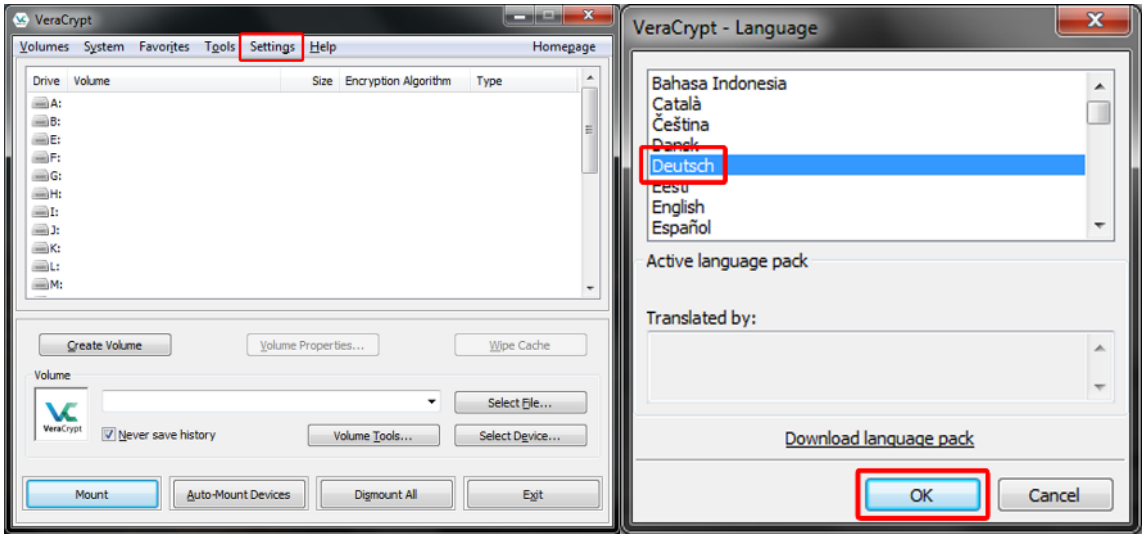


Schritt 2 – Mit VeraCrypt einen Kontainer erstellen

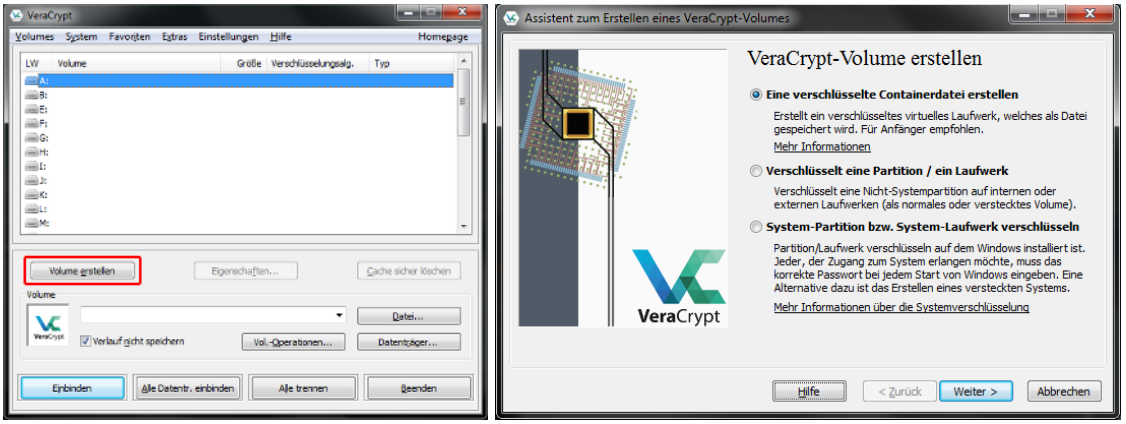
An dem Zielpfad, an dem das Programm extrahiert wurde, sollte sich nun die *VeraCrypt.exe* befinden. Führe die *exe-Datei* aus und starte damit das Programm.



Du solltest nun die englische Oberfläche des Programms sehen. Damit du diese auf Deutsch stellen kannst, wählst du unter *Settings* den Auswahlpunkt *Language…* aus. Anschließend solltest du die deutsche Oberfläche sehen.



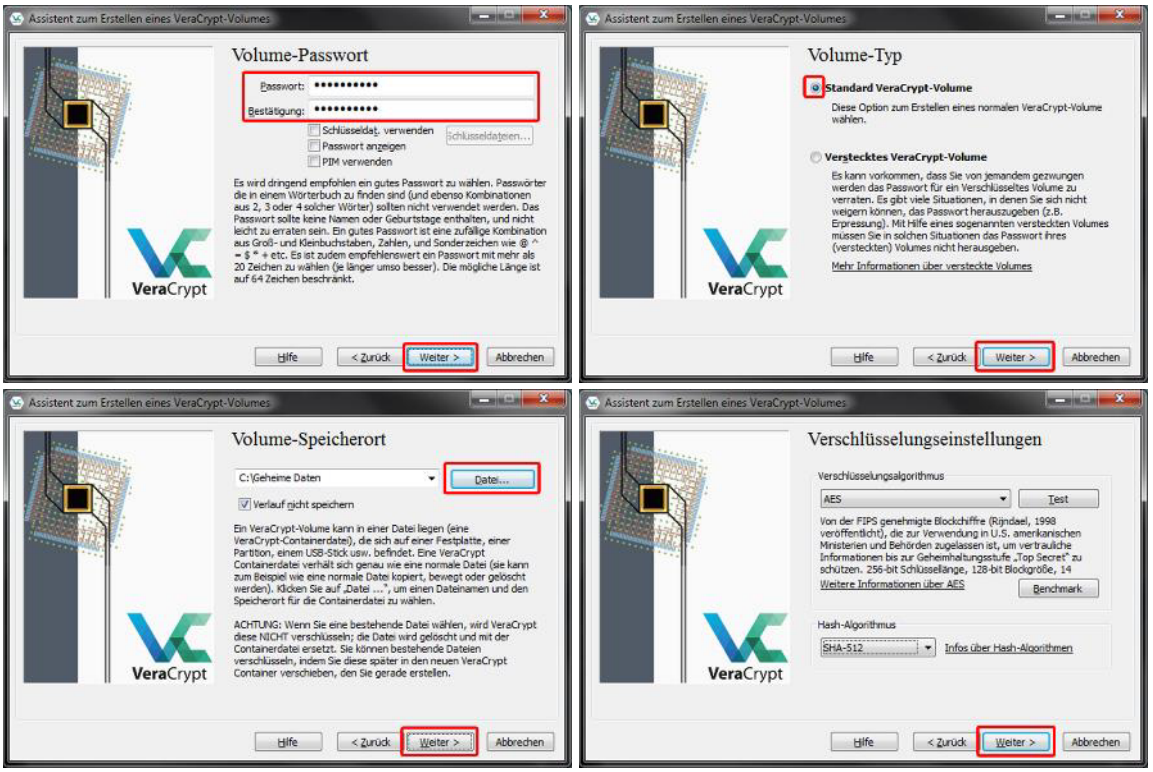
Um nun einen Kontainer zu erstellen musst du auf *Volume erstellen* klicken, woraufhin sich ein neues Fenster mit einem Assistenten zur Erstellung des Kontainers öffnet.



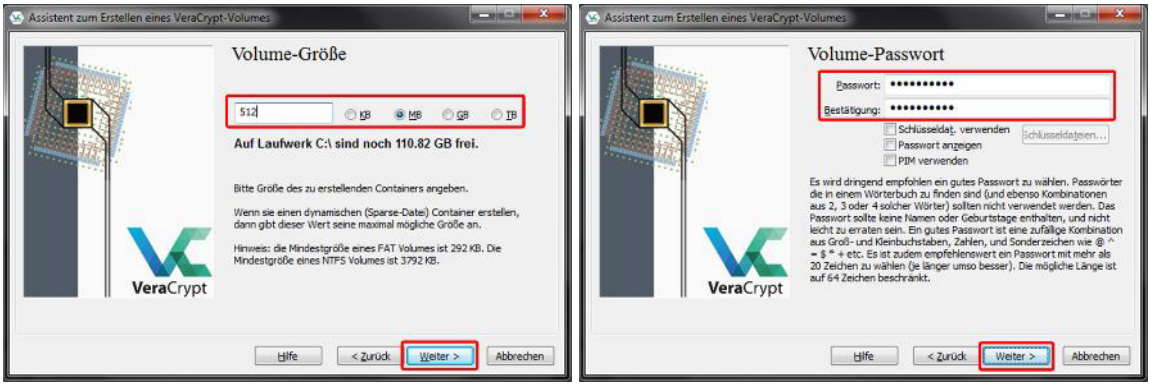
Diese Anleitung beschreibt den Assistenten nicht vollumfänglich, sondern geht sehr zügig durch die einzelnen Punkte. Bitte lies jede Seite des Assistenten ausführlich durch, bevor du

die von uns angegebenen Schritte ausführst. Beachte auch die Hinweise und Anmerkungen des Assistenten!

Wie bereits gesagt, wollen wir einen Kontainer und keine Partition oder gar das Systemlaufwerk verschlüsseln, wähle daher *Eine verschlüsselte Contrainerdatei erstellen* aus und klicke auf Weiter >. Wähle anschließend *Standard VeryCrypt-Volume* aus, da wir unseren Kontainer nicht auf dem System verstecken wollen. Danach musst du über *Datei…* einen Zielpfad für den Kontainer auswählen und kannst dann auf *Weiter* > klicken. Auf der anschließenden Seite kannst du das Verschlüsselungsverfahren auswählen.

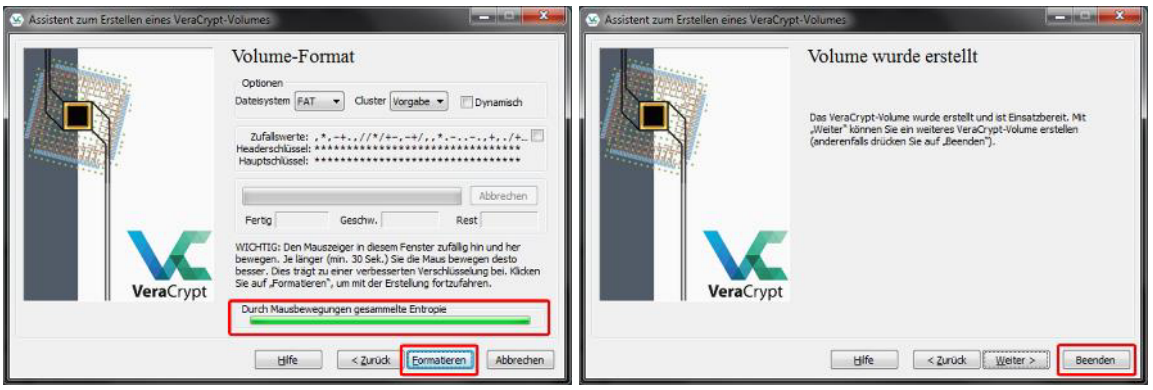


Belasse es zunächst beim Standard (AES mit SHA-512) und klicke auf *Weiter* >, um dann die Größe des Kontainers zu definieren. Für diese Anleitung verwendeten wir 512 MB. Klicke anschließend auf *Weiter* > und du wirst aufgefordert ein Passwort festzulegen. Trage in die entsprechenden Felder das Passwort ein und klicke auf *Weiter* >. Solltest du einen Hinweis bekommen, dass das Passwort kurz sei, dann wähle *Nein* um das Passwort zu ändern, oder *Ja* um trotzdem fortzufahren. (Für dieses Beispiel ist die Länge des Passworts ersteinmal egal.)



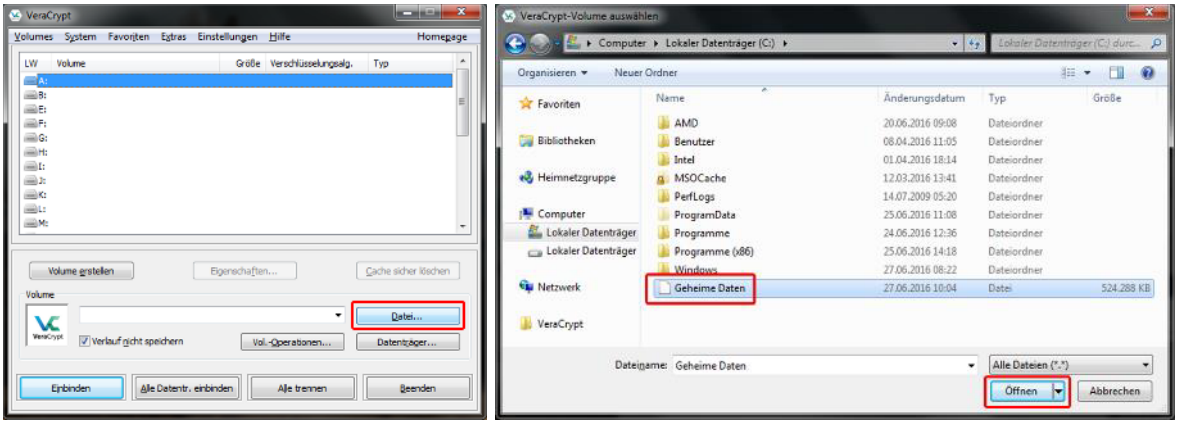
Auf der anschließenden Seite kannst du das Dateisystem des Kontainers auswählen sowie die Formatierung starten. Dafür musst du jedoch mit der Maus solange innerhalb des Fensters

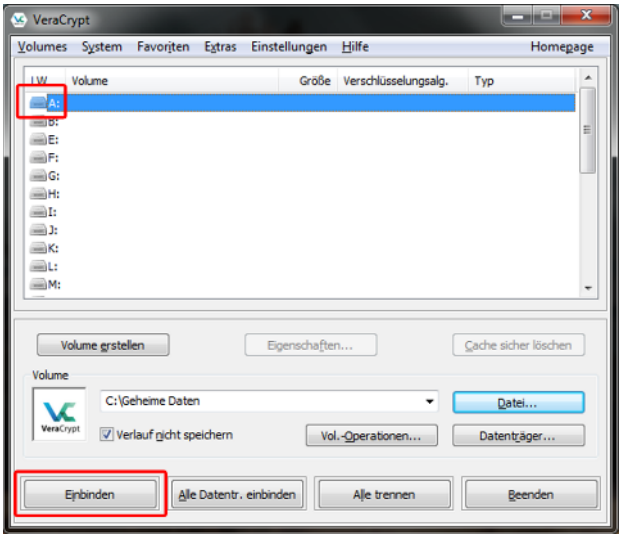
zufällige Bewegungen machen, bis die Leiste Durch *Mausbewegungen gesammelte Entropie* voll ist. Erst dann kannst du auf Formatieren klicken. Sobald der Kontainer erstellt wurde, kannst du den Assistenten mit *Beenden* beenden.

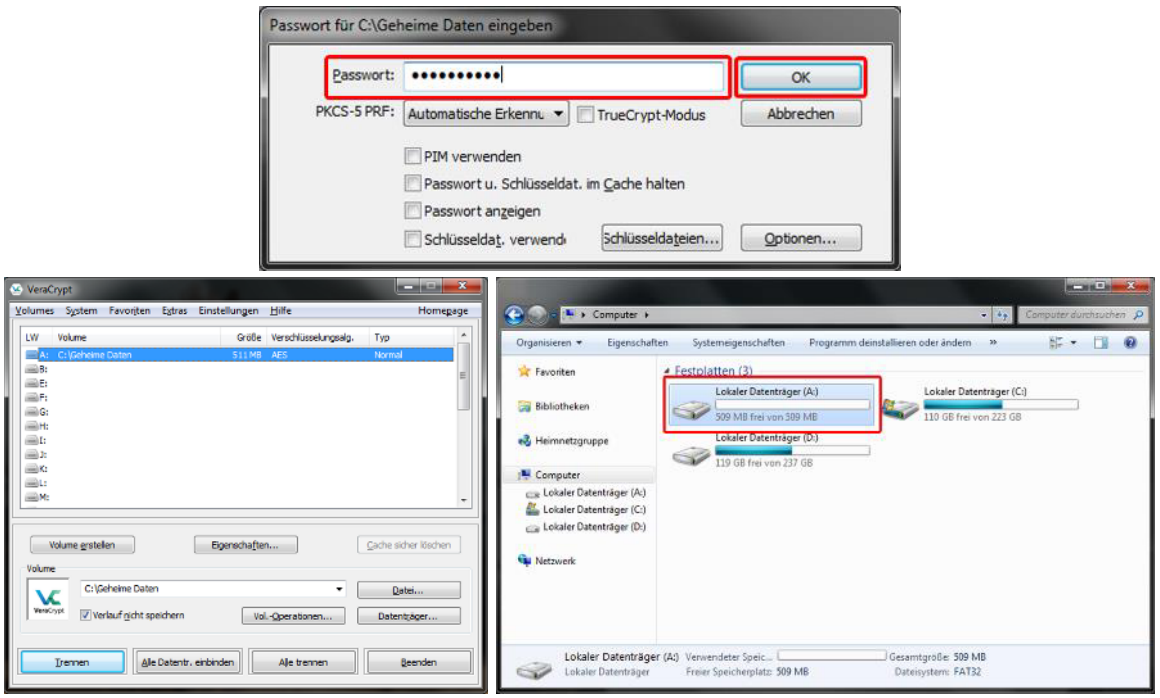


Schritt 3 – Kontainer einbinden

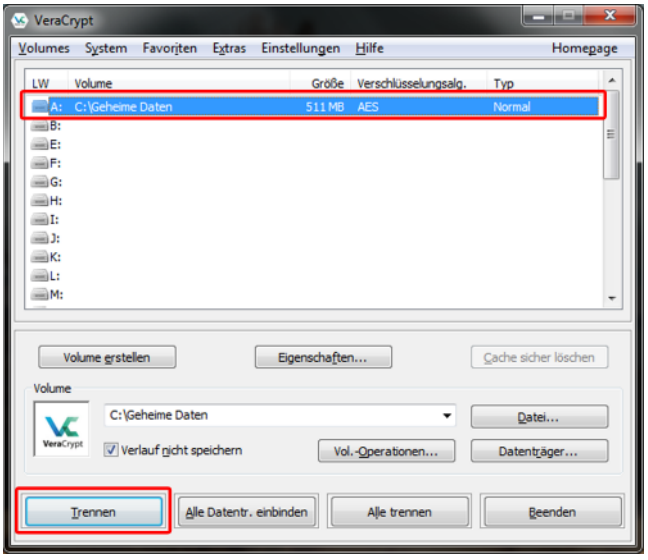
Um einen Kontainer nun einzubinden, das bedeutet, dass man Dateien dort ablegen und somit verschlüsseln lassen kann, musst du zunächst auf *Datei…* klicken und die entsprechende Datei des Kontainers auswählen. Anschließend kannst du ein Laufwerk aus der oberen Liste auswählen und mit *Einbinden* den Kontainer einbinden. Im Anschluss musst du nun das Passwort für den Kontainer eingeben und kannst dann sehen, dass der Container eingebunden wurde. Danach kannst diesen Kontainer wie ein ganz normales Laufwerk verwenden.







Zum Trennen des Kontainers (damit das Laufwerk nicht mehr verfügbar ist), kannst du diesen in der oberen Liste auswählen und auf *Trennen* klicken.



Vorsicht

Denke immer daran, dass wenn du einmal das Passwort vergessen hast, dann ist es sehr schwer bis garnicht möglich, die verschlüsselten Dateien wiederherzustellen. Dies ist gerade dann sehr ärgerlich, wenn du die Partition des Betriebsystems (also z. B. dein Windows) verschlüsselt hast. Verwende also immer sichere Passwörter, die du dir auch merken kannst. Wie das am besten geht, zeigt dir folgendes Beispiel:

Angenommen du brauchst ein sicheres Beispiel. Wähle ein Lied, Gedicht oder eine Stelle aus deinem Liebslingsbuch aus. Wir nehmen hier als Beispiel die erste Zeilen des Erlkönigs:

Wer reitet so spät durch Nacht und Wind?

Anschließend ersetzen wir bestimmte Buchstaben durch Zahlen. Zum Beipsiel *e* durch *3*, *i* durch *1*, *a* durch *4*, *s* durch *5*, *t* durch | und *o* durch *0*. Dann erhalten wir:

W3r r31|3< 50 5pä| durch N4ch| und W1nd?

Danach ersetzen wir bestimmte Buchstaben oder Wörter durch Sonderzeichen. Zum Beispiel *und* durch &, c durch < und n durch /\/:

W3r r31|3| 50 5pä| dur<h /\/4<h| & W1/\/d?

Zum Abschluss entfernt man alle Leerzeichen und erhält es sehr sicheres Passwort:

W3rr31|3|505pä|dur<h/\/4<h|&W1/\/d?

Natürlich bedarf es etwas Übung, bis man es ohne große Mühe am Stück eingeben kann.

Substitution – Teil 1

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Substitution* beschreiben. Bei der Substitution werden Buchstaben oder sogar ganze Wörter des Klartextes durch andere Buchstaben, Wörter oder auch Symbole ersetzt. Ein Beispiel, das euch vielleicht bereits bekannt ist, stellt die Caesar-Verschlüsselung dar. Es gibt jedoch auch noch die Verschlüsselung nach Atbash und mittels Polybius-Tafel.

Atbash- und Ceasar-Verschlüsselung

Bei beiden Verschlüsselungen werden die Buchstaben des Alphabetes durch andere Buchstaben ausgetauscht. Dies kann jedoch auf auf verschiedene Arten erfolgen.

So wird bei Atbash der erste Buchstabe des Alphabetes mit dem Letzten, der Zweite mit dem Vorletzten und so weiter ausgetauscht.

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

Anders erfolgt bei Caesar eine Verschiebung des Alphabetes. Hier wird jeder Buchstabe mit dem Buchstaben ersetzt, der um einen festen Wert später im Alphabet auftaucht.

Klaralphabet																								
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
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
Caesar Geheimalphabet mit einer Verschiebung von 6																								

Aufgabe 1

Verschlüssle die folgende Nachrichten mit Atbash:

TREFFEN UM DREI

Aufgabe 2

Entschlüssle die folgende Nachricht mit Atbash:

WVI TVRVI SZG WRV YVFGV

Verschlüsselung mittels Polybius-Tafel

Die Buchstaben eines Klartextes müssen jedoch nicht immer nur durch Buchstaben ersetzt werden. Es ist auch möglich sie durch Zahlen zu ersetzen, wie das Verfahren mittels Polybius-Tafel zeigt.

Die Polybius-Tafel stellt eine Art Tabelle (oder auch Matrix genannt) dar, in der jeder Buchstaben des Alphabets eingetragen wird und eine X- und Y-Koordinate erhält.

		Y				
		1	**2**	**3**	**4**	**5**
X	**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

Die Anzahl der Zeilen und Spalten kann dabei beliebig angepasst werden. Im obigen Beispiel wird nun das A mit „1 1“, „11“ bzw. „1,1“ oder B mit „1 2“, „12“ bzw. „1,2“ verschlüsselt (für die Schreibweise der Koordinaten gibt es noch etliche weitere Möglichkeiten).

Aufgabe 3

Verschlüssle die Nachricht aus Aufgabe 1 mittels der obigen Polybius-Tafel.

Aufgabe 4

Entschlüssle die folgende Nachricht:

14 15 42

43 13 23 31 45 15 43 43 15 31

31 24 15 22 44

11 32

21 31 45 43 43

Transposition

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Transposition* beschreiben. Bei der Transposition werden (meist) Buchstaben des Klartextes so verschoben, dass die eigentlich Nachricht nicht mehr direkt lesbar ist. Dabei kann es vorkommen, dass zusätzliche Gegenstände zum Entschlüsseln notwendig sind (siehe Skytale), dies ist aber nicht zwingend der Fall (siehe fleißnersche Schablone, Gartenzaun oder Krebs-Verfahren).

Skytale-Verschlüsselung

Bei der Skytale-Verschlüsselung wird ein Holzstab (der sogenannte Skytale) mit einem bestimmten Durchmesser verwendet. Um diesen Holzstab wird dann das Papier (oder damals Leder) herumgewickelt und darauf geschrieben (siehe rechtes Bild). Der Durchmesser ist der Schlüssel.

Aufgabe 1

Verschlüssle die folgende Nachricht mit einer der bereitgestellten Skytales:

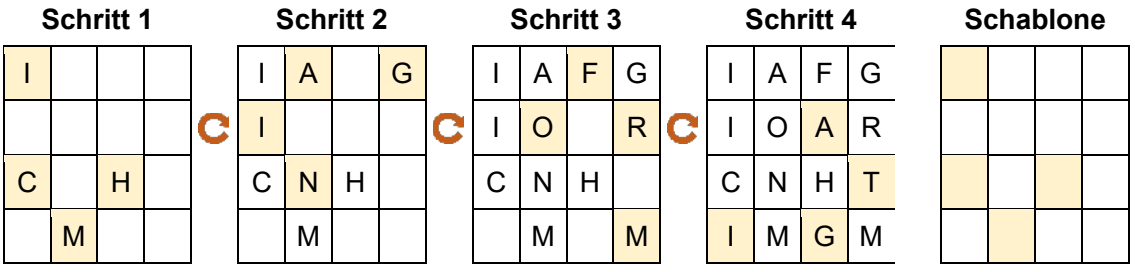
Austausch heute Abend am bekannten Ort

Aufgabe 2

Suche dir eine Partnerin oder einen Partner und verschlüsselt jeweils eine Nachricht mit einen der bereitgestellten Skytales.

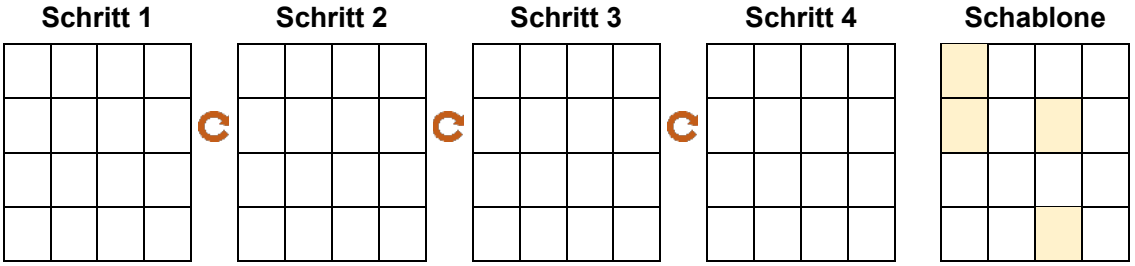
Verschlüsselung mittels fleißnersche Schablone

Ein anderes Hilfsmittel stellt die fleißnersche Schablone dar (die nicht zwingend physisch vorhanden sein muss). Der Klartext wird hier in eine Art Tabelle bzw. Matrix geschrieben, wobei eine Schablone vorgibt, wo etwas eingetragen werden darf. Sind alle erlaubten Felder genutzt, wird die Schablone mit oder gegen den Uhrzeigersinn (aber immer einheitlich) gedreht und der verbleibende Text mittels Schablone eingetragen. Das folgende Beispiel zeigt wie der Text „Ich mag Informatik“ verschlüsselt wird. Die gelben Kästchen geben die erlaubten Felder der Schablone an.



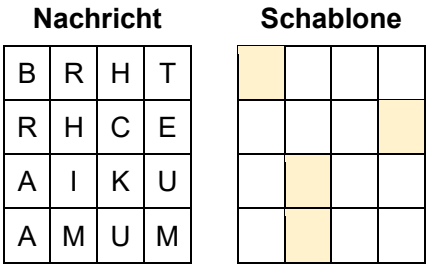
Aufgabe 3

Verschlüssle einen Satz mittels fleißnerscher Schablone.



Aufgabe 4

Entschlüssle die folgende Nachricht.



Substitution – Teil 2

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Substitution* beschreiben. Weiter gibt es aber auch noch die Unterteilung in *Mono-* und *Polyalphabetisch*. Bei Ersterem findet nur ein Alphabet verwendung (siehe Caesar- oder Atbash-Verschlüsselung), was das „Knacken“ mittels einer Häufigkeitsanalyse einfach ermöglicht. Bei polyalphabetischen Verfahren werden mehrere Geheimalphabete verwendet und somit gleiche Buchstaben durch mehrere verschiedene Buchstaben ersetzt. Ein Beispiel für ein solches Verfahren ist die Vigenére-Verschlüsselung.

Vigenére-Verschlüsselung

Dieses Verfahren ähnelt der Caesar-Verschlüsselung, nur mit dem Unterschied, dass man hier nicht ein Geheimalphabet (das verschobene Alphabet) verwendet, sondern mehrere. Damit die Person, die die Nachricht verschlüsselt und die Person, die die Nachricht entschlüsselt, wissen welche und wieviele Geheimalphabete verwendet werden, einigen sie sich auf ein *Schlüsselwort*.

Die Positionen der einzelnen Buchstaben des Schlüsselwortes im Alphabet geben an, um wieviel das Alphabet verschoben wird. Die Anzahl der Geheimalphabete entspricht dabei der Länge des Schlüsselwortes. Wird zum Beispiel das Schlüsselwort *GEHEIM* verwendet, dann werden zum Verschlüssel des Klartextes sechs Geheimalphabete verwendet:

1. Geheimalphabet ist das Alphabet um **sechs** Buchstaben verschoben.
2. Geheimalphabet ist das Alphabet um **vier** Buchstaben verschoben.
3. Geheimalphabet ist das Alphabet um **sieben** Buchstaben verschoben.
4. Geheimalphabet ist das Alphabet um **vier** Buchstaben verschoben.
5. Geheimalphabet ist das Alphabet um **acht** Buchstaben verschoben.
6. Geheimalphabet ist das Alphabet um **zwölf** Buchstaben verschoben.

Die Tabelle auf der folgenden Seite veranschaulicht dies nochmal für alle Buchstaben.

Soll nun der Text *ICH MAG INFORMATIK* verschlüsselt werden, dann wir der erste Buchstabe (I) mit dem ersten Geheimalphabet verschlüsselt, der zweite mit dem zweiten und so weiter, bis man wieder beim ersten Geheimalphabet anfängt:

I	$\xrightarrow{G}$	O	I	$\xrightarrow{G}$	O	A	$\xrightarrow{G}$	G
C	$\xrightarrow{E}$	G	N	$\xrightarrow{E}$	R	T	$\xrightarrow{E}$	X
H	$\xrightarrow{H}$	O	F	$\xrightarrow{H}$	M	I	$\xrightarrow{H}$	P
M	$\xrightarrow{E}$	Q	O	$\xrightarrow{E}$	S	K	$\xrightarrow{E}$	O
A	$\xrightarrow{I}$	I	R	$\xrightarrow{I}$	Z			
G	$\xrightarrow{M}$	S	M	$\xrightarrow{M}$	Y			

Aus „ICH MAG INFORMATIK“ wird also „OGO QIS ORMSZYGXPO“.

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

Aufgabe 1

Verschlüssle die folgende Nachricht mit der Vigenére-Verschlüsselung und dem Schlüsselwort GEHEIM:

TREFFEN UM DREI

Aufgabe 2

Entschlüssle die folgende Nachricht mit dem Schlüsselwort GEHEIM.

JIY KMUKV OEB POI IICFK

Vigenére knacken

Das Knacken der Vigenére-Verschlüsselung ist nicht so einfach wie bei der Caesar-Verschlüsselung, jedoch ähnlich, da auch hier eine Häufigkeitsanalyse stattfindet. Die Schwierigkeit ist aber, auf das Schlüsselwort zu kommen. Hier gibt es Möglichkeiten, die das Ermitteln des Schlüsselwortes überaus schwierig gestalten. Zunächst sollen jedoch einfache Schlüsselwörter betrachtet werden, um das Vorgehen einmal grundlegend zu verstehen.

Es sind drei Schritte notwendig, um die Verschlüsselung zu knacken:

1. Wiederkehrende Buchstabenfolgen im verschlüsselten Text werden gesucht.
2. Anschließend wird hiermit die Länge des Schlüsselwortes ermittelt.
3. Letztlich erfolgt dann die Bestimmung des Schlüsselwortes.

Wie aber auch schon bei der Häufigkeitsanalyse bei Caesar, fällt das Knacken leichter, wenn der Geheimtext sehr lang ist. Also wenn man eine große Datengrundlage benutzt.

Schritt 1: Wiederkehrende Buchstabenfolgen suchen

Der Geheimtext wir zunächst auf wiederkehrende Buchstabenfolgen untersucht. Diese sollten im Idealfall eine Mindestlänge von drei Buchstaben haben und innerhalb des Textes markiert werden. Die Buchstabenfolgen zeigen mit hoher Wahrscheinlichkeit, die gleichen Buchstaben des Geheimalphabets, mit dem verschlüsselt wurde. Das bedeutet, dass häufig vorkommende Buchstabenfolgen innerhalb des Geheimtextes auf häufig vorkommende Buchstabenfolgen (z. B. ein, der, die, das, sch …) aus der deutschen Sprache beruhen.

```
ETYJANSDUVYECVPRIDEIIYPMNQLGHPCXEIERINSXIXXIRLMIRPDAICOIIYQECSPVWP
YRETYWOWNLETYJANSIREPBTQZPGPYZOYMYCSDXAMPRBPDMTKEHIPTQMPCAIPOIRVZQ
MPYSBOTISPCIIYQECSEIXEYYNPTRFLNLZFVRANVINTDXWTCHSTNLZPTKEYLFECOMED
PVETYJANSITPIXIDEWINSIRPTRFLNLECKYKYLGKPYELDLRDPCIETYJANSITPIXEPTR
ETYJANSIRDNLLFPWSPWQANSXEDLYCSPMNQLGHPCIIYPRETYJANSINEPBTKFONLNOEY
ZFETYJANSSDPCRINSXETYJANSHIPDIRPTRFLNLEEPBTHTVDOTGHDTGHPCJOCOIRY
```

Schritt 2: Länge des Schlüsselwortes ermitteln

Nun wird für jede Buchstabenfolge ermittelt, wie groß der Abstand vom ersten Buchstaben der Buchstabenfolge zum erneuten Auftreten der Folge ist. Zum Beispiel wäre für XYZ der Abstand innerhalb von AA**XYZ**AAAA**XYZ**AAAAAA**XYZ**AA einmal Sieben und einmal Neun.

Aus der Tatsache, dass wiederkehrende Buchstabenfolgen innerhalb des Geheimtextes auf gleichen Buchstabenfolgen innerhalb des Klartextes zurückzuschließen sind, ergibt sich, dass die Länge des Schlüsselwortes ein Teiler des oben erwähnten Abstandes sein muss.

Das bedeutet, dass nun für jeden Abstand geschaut werden muss, welche Teiler dieser besitzt und welcher Teiler für alle Buchstabenfolgen in Frage kommen. Orientierung kann hier der ggT (größte gemeinsame Teiler) der einzelnen Abstände bieten. Wenn ein oder mehere Teiler gefunden wurden, dann wird die Länge des Schlüsselwortes einem davon entsprechen. Wenn mehrere Teiler in Frage kommen, muss Schritt 3 gegebenenfalls mehrfach durchgeführt werden, bis das Schlüsselwort ermittelt wurde.

Buchstabenfolge	Abstand vom ersten Buchstaben zum ersten Buchstaben	ggT der Abstände pro Buchstabenfolge
ETYJANS	$76 = 2^2 * 19$, $124 = 2^2 * 31$, $48 = 2^4 * 3$, $60 = 2^2 * 3 * 5$, $24 = 2^2 * 3$, $16 = 2^4$	2^2
IIY	$36 = 2^2 * 3^2$, $88 = 2^3 * 11$, $160 = 2^6 * 5$	2^2
NLE	$152 = 2^3 * 19$, $140 = 2^2 * 5 * 7$	2^2
PTRFL	$64 = 2^6$, $140 = 2^2 * 5 * 7$	2^2

Schritt 3: Schlüsselwort ermitteln

Da nun bekannt ist, wie Lang das Schlüsselwort ist, kann eine Häufigkeitsanalyse angewendet werden. Dafür wird der Text in Abschnitte von der Länge des Schlüsselwortes unterteilt. Da bei Vigenére der erste, zweite, dritte usw. Buchstabe eines solchen Abschnitts immer mit dem ersten, zweiten, dritten usw. Geheimalphabet verschlüsselt wurde, muss nun ermittelt werden, welcher Buchstabe innerhalb dieser Menge an Buchstaben am häufigsten vorkommt. Angenommen für den ersten Buchstaben des Schlüsselwortes ergibt sich, dass X am häufigsten verschlüsselt wurde, dann ist der Buchstabe gesucht, mit dem das E auf X abgebildet wird.

```
ETYJ ANSD UVYE CVPR IDEI IYPM NQLG HPCX EIER INSX IXXI RLMI RPDA
ICOI IYQE CSPV WPYR ETYW OWNL ETYJ ANSI REPB TQZP GPYZ OYMY CSDX
AMPR BPDM TKEH IPTQ MPCA IPOI RVZQ MPYS BOTI SPCI IYQE CSEI XEYY
NPTR FLNL ZFVR ANVI NTDX WTCH STNL ZPTK EYLF ECOM EDPV ETYJ ANSI
TPIX IDEW INSI RPTR FLNL ECKY KYLG KPYE LDLR DPCI ETYJ ANSI TPIX
EPTR ETYJ ANSI RDNL LFPW SPWQ ANSX EDLY CSPM NQLG HPCI IYPR ETYJ
ANSI NEPB TKFO NLNO EYZF ETYJ ANSS DPCR INSX ETYJ ANSH IPDI RPTR
FLNL EEPB THTV DOTG HDTG HPCJ OCOI RY
```

Buchstabe des Schlüsselwortes	Vorkommende Buchstaben mit ihrer Häufigkeit	Vermuteter Buchstabe des Schlüsselwortes
1. Buchstabe	**E** = 18, I = 14, A = 11, R = 8, …	E $\xrightarrow{A}$ E
2. Buchstabe	**P** = 24, N = 13, T = 12, Y = 9, …	E $\xrightarrow{L}$ P
3. Buchstabe	**Y** = 15, S = 12, P = 11, T = 10, …	E $\xrightarrow{U}$ Y
4. Buchstabe	**I** = 19, R = 12, J = 9, X = 8, …	E $\xrightarrow{E}$ I

In dem aufgeführten Beispiel ergibt sich also, dass das Schlüsselwort „ALUE“ sein soll. Das dieses Verfahren nicht immer auf anhieb den richtigen Schlüssel ergibt, lässt sich dann erkennen, wenn man versucht mit diesem Schlüsselwort zu ermitteln. Das eigentlich Schlüsselwort lautete nämlich „ALLE“ und das Verfahren zum Knacken der Verschlüsselung hätte sicherlich besser geklappt, wenn die Nachricht länger ist.

Entschlüsselt man nun den Text ergibt sich:

EINFACH ZU KNACKEN IST EIN EINFACHER TEXT NICHT IMMER ABER ES WIRD EINFACHER WENN EIN SOLCH EINFACHER TEXT FOLGEN VON BUCHSTABEN BESITZT DIE IMMER WIEDERKOMMEN

OB DIESER EINFACH TEXT NUN EINFACH ZU KNACKEN IST WIRD SICH ZEIGEN

ABER DIESER EINFACHE TEXT IST SICHER EINFACHER ZU KNACKEN ALS ANDERE EINFACHE TEXTE

EIN EINFACHER SCHLUESSEL MACHT ES AUCH EINFACHER EINEN EINFACHEN TEXT ZU KNACKEN

OB EINFACH ODER NICHT EINFACH DIESER EINFACHE TEXT WIRD DICH SICHER FORDERN

Aufgabe 1

Knacke die Verschlüsselung anhand des folgenden Textes und entschlüssle die ersten Zeilen des Geheimtextes[1]:

PWTMYTBADKDGPWPFYWFGUESOTLUPNVYWAPKCSOOJWWASTLSUZUSJMJBBRS
TIMGPYSXOJWWASMMZQLCHJQWGYDHKOJWWASTMFPADWIPVKLHONZWPDPWRA
AGQPRKNJCNPKGPJJLTHYOWOHPGYJWCUEKUZLGAOWKHOGPESMZMRWPBKVFV
ZTQNLAGSFSMVWTDPWRAAGQPRKNJCNPTGTKEOMSGVLYVCHKBVKLOFOBLGNC
IVXWPLYBZAAEOOWKEWEODZKZOGPWGOMSWMPWTIFFLCTUTYGUOSLZSILYOH
EWEODSRVVYHSFAVVHHWGIPTGHYHCWJVLERGJWKPDHGJWTUTQNBXGZEUKTW
IAZPPMOGPWGJQWGYDHKNJCNPSOVWTZPFOMNQUQFGOWPYTQNBAIVOSXNSNZ
NVHMSPAHCXBWVDTFJRWFLASXAGPHYHCWJVLEOANWKUPTXIYGUFFSQLLHZR
KZFGPYTXIYGUOWKVAEOEAOBBCVOSXVWKUMSGVLYVCHKBOGYOSTSGGUYSTA
APKYWIPLBBRSRIKULYJUVWKUPFHMDKLMWMMFRLCGUVKQSWAGVVWYNVLZSI
LYROMKKJSBAZSWMOWKHMILSCKZAIRPWZHMGPYSXLWTNCIVXWPIPNOMZGUS
SXIMUIPYUUEGUKICMDEOPFMZMRWPGOMYGOZSXBOKLGWKTWHYLUKVEWZDAG
VEKUOSYBWPZDHKTDGUFBJEWNJSSLZSILYYUMFPAPAGVKVLWZKV

Tipp: Von den interessanten Buchstabenfolgen wurde das erste Vorkommen bereits markiert. In Schritt 2 sollte nicht nur auf den ggT geachtet werden, sondern eher auf alle vorkommenden Teiler.

Buchstabenfolge	Abstand vom ersten Buchstaben zum ersten Buchstaben	ggT der Abstände pro Buchstabenfolge
OJWWAS		

[1] QUELLE: http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.2_Vigenere/AB%20Vigenere%20knacken.pdf

TXIYGU		
YHCWJVLE		
QPRKNJ		
AEO		
PWT		

Buchstabe des Schlüsselwortes	Vorkommende Buchstaben mit ihrer Häufigkeit	Vermuteter Buchstabe des Schlüsselwortes
1. Buchstabe		E →
2. Buchstabe		E →
3. Buchstabe		E →

Das Schlüsselwort lautet: _____

Die ersten Zeilen des Klartextes lauten:

_____

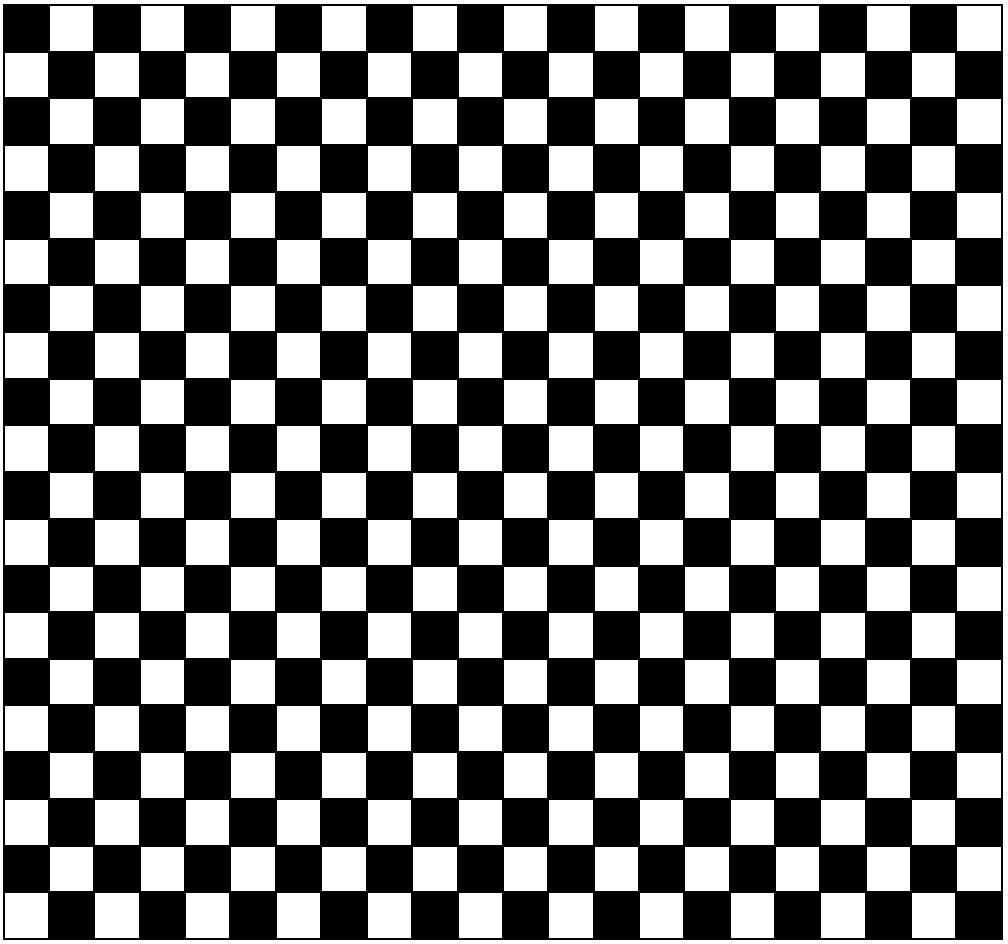
_____

_____

_____

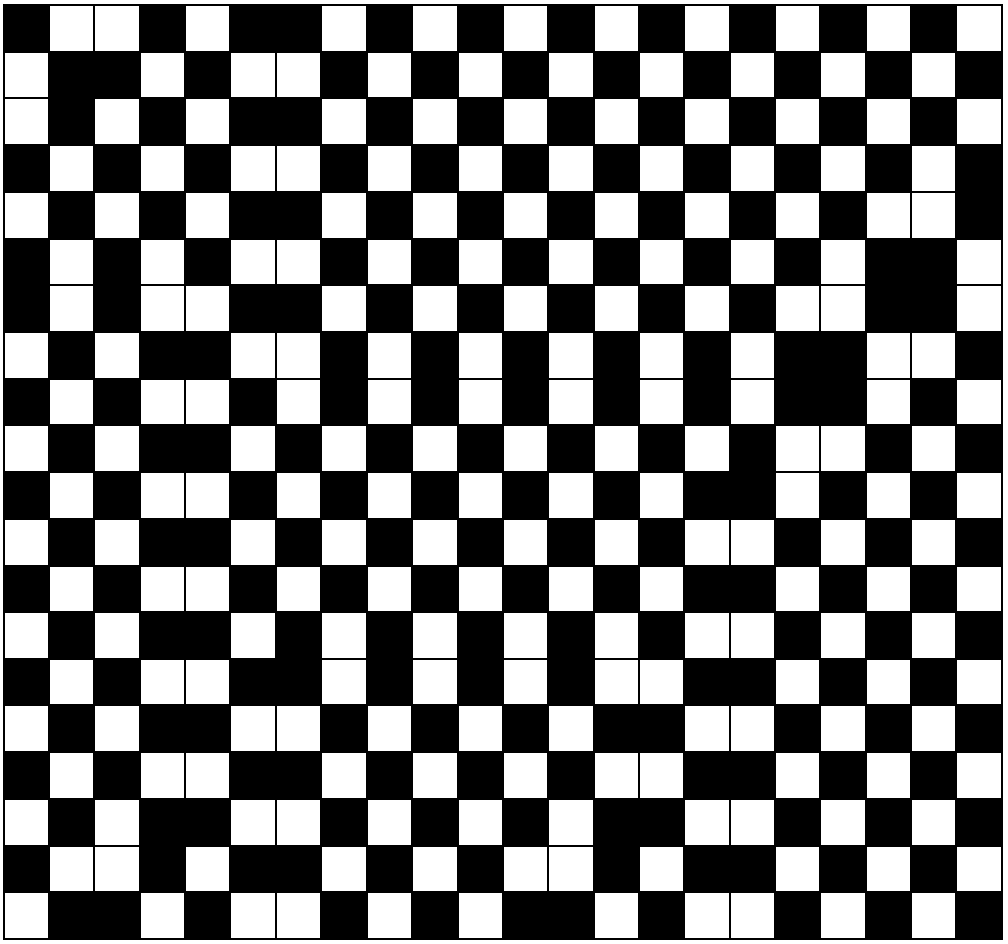
Zu Aufgabe 4

Bitte diese Seiten auf Folie ausdrucken.



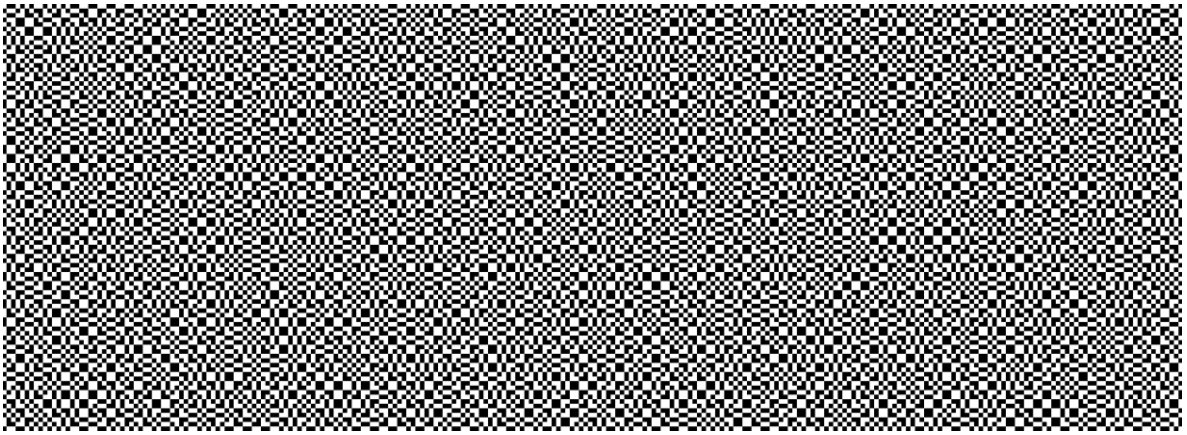
Zu Aufgabe 4

Bitte diese Seiten auf Folie ausdrucken.



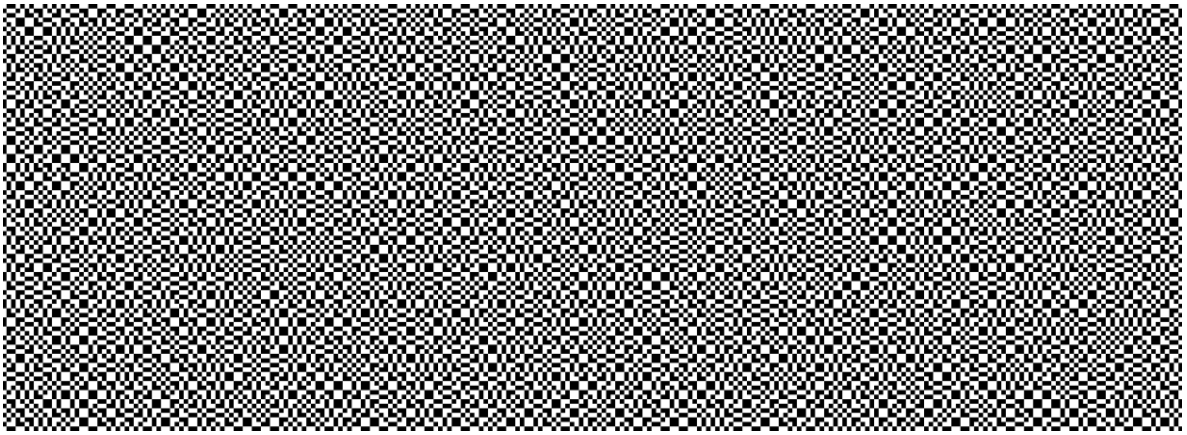
Zu Aufgabe 4

Bitte diese Seiten auf Folie ausdrucken.



Zu Aufgabe 4

Bitte diese Seiten auf Folie ausdrucken.



Steganographie

Um Informationen sicher zu Übertragen ist es manchmal sinnvoll, dass die Nachricht gar nicht erst den Anschein macht, dass es sich hierbei um eine verschlüsselte Nachricht handelt.

Angenommen Alice sitzt nach einem lohnenswerten Geldraub im Gefängnis und möchte Bob eine Nachricht schicken, um ihm den Ort des versteckten Geldes mitzuteilen. Sie könnte zwar diese Nachricht sehr gut verschlüsseln, was zur Folge hat, dass die daraus resultierende Nachricht zwar nicht vom Gefängniswärter Walter entschlüsselt wird, aber vermutlich würde dieser die Nachricht dann auch nicht an Bob weiterleiten. Also schreibt Alice lieber ein (belangloses) Liebesgedicht, bei dem die Anfangs- und/oder Endbuchstaben der Zeilen hintereinander gelesen die eigentliche Nachricht bilden, die dann von Walter wahrscheinlicher an Bob weitergeleitet wird.

Dieses Themenfeld, bei denen die Verschleierung von Informationen im Vordergrund stehen, nennt man Stenographie. Hierbei gibt es viele verschiedene Verfahren, die mit ganz unterschiedlichen Hilfsmittel funktionieren.

Einfache Beispie

Aus der Geschichte gibt es viele einfache Beispiele, wie Geheimtinte (Zitronensaft) oder doppelte Böden in Briefumschlägen, Schubladen etc. Weitere aufwendigere Verfahren sind zum Beispiel Mikrofilme (bekannt aus alte Agentenfilmen) oder Wasserzeichen (Machine Identification Codes).

Aufgabe 1

Informiere dich über die obigen Beispiele im Internet und fasse diese kurz zusammen.

Linguistische Verfeinerungen

Abseits der verwendenten Hilfsmittel wie Tinte oder doppelte Böden, gibt es auch Verfahren, die mehr mit der Sprache und Codierung ebendieser arbeiten. Ein Beispiel hierfür ist das obige Liebesgedicht von Alice an Bob. Um jedoch auch andere Mittel als nur die gängige Sprache zu nutzen, müssen Informationen codiert werden. Damit wiederum solche Codierungen nicht auffallen, werden diese in sogenannte Semagramme eingebettet. Hierbei handelt es sich um Bilder, Melodien etc. in denen kleine Details, die in Wirklichkeit die codierten Geheiminformationen darstellen, enthalten. Im digitalen Bereich können dies auch ein paar zusätzliche Bytes innerhalb einer MP3 oder eines Bildes sein, die an der ursprünglichen Melodie oder dem Bild nichts ändern.

Aufgabe 2

Betrachte das Beispiel und versuche herauszufinden, wie die Informationen verschleiert wurden. Die verschleierte Nachricht lautete: Um drei am Treffpunkt.

Aufgabe 3

Versuche nun selbst mittels einer beliebigen Methode eine Nachricht bzw. Information zu verschleiern.

Visuelle Kryptographie

Einzeln betrachtet lässt sich den Folien kein Sinn entnehmen, aber was passiert, wenn man sie übereinander legt? (Wie das Verfahren funktioniert lässt sich am leichtesten mit dem groben händisch erstellten Raster erkennen.)

Aufgabe 4

Versuche zu beschreiben, wie die visuelle Kryptographie funktioniert und erstelle ein eigenes Beispiel auf einer neuen Folie. Du kannst die einfache Karofolie als Gegenstück verwenden.

Musterlösungen

A2.8

Aufgabe 1

GIVUUVM FN WIVR

Aufgabe 2

DER GEIER HAT DIE BEUTE

Aufgabe 3

63 43 51 61 61 51 72 (= TREFFEN)
73 62 (= UM)
41 43 51 22 (= DREI)

Aufgabe 4

DER SCHLUESSEL LIEGT AM FLUSS

A2.9

Aufgabe 1

Die Lösungen sind abhängig von der Anzahl der Flächen, die der Skytale besitzt. Hier mögliche Lösungen:

Anzahl der Flächen	Nachricht
4	AAHTEMAETUUHENBNNSSEADENOTCUBAKTR
5	AUEBMNOUSUEBNRSCTNETTTHEDKEAHAAAN
6	ASTDAOUCEANRSHAMNTTHBBTAEEEEUUNKN
7	ACABEUHBENSHEKOTENARAUDNTUTANSEMT
8	AHEATUHNNSEDNTUATATMEUEBNSAEOCBKR

Aufgabe 4 - BEI MARK UM ACHT UHR

A2.10

Aufgabe 1 - ZVLJNQT BQ PXIP

Aufgabe 2 - DER GEIER HAT DIE BEUTE

A2.11

Aufgabe 1

Schritt 1

PWTMYTBADKDGPWPFYWFGUESOTLUPNVYWAPKCSOOJWWASTLSUZUSJMJBBRS
TIMGPYSXOJWWASMMZQLCHJQWGYDHKOJWWASTMFPADWIPVKLHONZWPDPWRA
AGQPRKNJCNPKGPJJLTHYOWOHPGYJWCUEKUZLGAOWKHOGPESMZMRWPBKVFV
ZTQNLAGSFSMVWTDPWRAAGQPRKNJCNPTGTKEOMSGVLYVCHKBVKLOFOBLGNC
IVXWPLYBZAAEOOWKEWEODZKZOGPWGOMSWMPWTIFFLCTUTYGUOSLZSILYOH
EWEODSRVVYHSFAVVHHWGIPTGHYHCWJVLERGJWKPDHGJWTUTQNBXGZEUKTW
IAZPPMOGPWGJQWGYDHKNJCNPSOVWTZPFOMNQUQFGOWPYTQNBAIVOSXNSNZ
NVHMSPAHCXBWVDTFJRWFLASXAGPHYHCWJVLEOANWKUPTXIYGUFFSQLLHZR
KZFGPYTXIYGUOWKVAEOEAOBBCVOSXVWKUMSGVLYVCHKBOGYOSTSGGUYSTA
APKYWIPLBBRSRIKULYJUVWKUPFHMDKLMWMMFRLCGUVKQSWAGVVWYNVLZSI
LYROMKKJSBAZSWMOWKHMILSCKZAIRPWZHMGPYSXLWTNCIVXWPIPNOMZGUS
SXIMUIPYUUEGUKICMDEOPFMZMRWPGOMYGOZSXBOKLGWKTWHYLUKVEWZDAG
VEKUOSYBWPZDHKTDGUFBJEWNJSSLZSILYYUMFPAPAGVKVLWZKV

Schritt 2

Buchstabenfolge	Abstand vom ersten Buchstaben zum ersten Buchstaben	ggT der Abstände pro Buchstabenfolge
OJWWAS	$28 = 2^2 * 7$ $21 = 3 * 7$	7
TXIYGU	$21 = 3 * 7$	/
YHCWJVLE	$119 = 7 * 17$	/
PRKNJ	$77 = 7 * 11$	/
AEO	$238 = 2 * 7 * 17$	/
PWT	$266 = 2 * 7 * 19$	/

Schritt 3

Buchstabe des Schlüsselwortes	Vorkommende Buchstaben mit ihrer Häufigkeit	Vermuteter Buchstabe des Schlüsselwortes		
1. Buchstabe	**P** = 21, Y =12, …	E	L →	P
2. Buchstabe	**S** = 26, W = 13, …	E	O →	S
3. Buchstabe	**K** = 20, G = 10, O = 10, X = 10, …	E	G →	K
4. Buchstabe	V = 16, **M** = 15, Z = 11, …	E	I →	M
5. Buchstabe	**W** = 24, J = 10, …	E	S →	W
6. Buchstabe	**G** = 25, P = 12, …	E	C →	G
7. Buchstabe	**L** = 18, U = 15, …	E	H →	L

Der entschlüsselte Text lautet:

EINE GRUPPE VON PERSONEN TEILT SICH SO IN DREI GRUPPEN DASS JEDER ZU GENAU EINER GRUPPE GEHOERT DIE ERSTE GRUPPE NENNT SICH DIE WAHREN WEIL SIE JEDE FRAGE WAHRHEITSGEMAESS BEANTWORTET DIE ZWEITE GRUPPE NENNT SICH DIE LUEGNER WEIL SIE JEDE FRAGE FALSCH BEANTWORTET DIE DRITTE GRUPPE NENNT SICH DIE WECHSLER WEIL SIE AUFEINANDERFOLGENDE FRAGEN ABWECHSELND WAHR UND FALSCH BEANTWORTET DABEI IST ABER NICHT FESTGELEGT OB JEWEILS DIE ERSTE FRAGE EINER SERIE VON FRAGEN RICHTIG ODER FALSCH BEANTWORTET WIRD JEDE PERSON ANTWORTET AUF EINE FRAGE NUR MIT JA ODER NEIN FRAGEN DIE NICHT MIT JA ODER NEIN BEANTWORTET WERDEN KOENNEN SIND NICHT ZUGELASSEN VON EINER BELIEBIGEN PERSON SOLL MAN DURCH FRAGEN DIE SICH NUR AUF DIE ZUGEHOERIGKEIT ZU EINER DER GRUPPEN BEZIEHEN HERAUS BEKOMMEN ZU WELCHER GRUPPE SIE GEHOERT WIE VIELE FRAGEN MUSS MAN MINDESTENS STELLEN UND WELCHE FRAGEN KOENNTE MAN STELLEN