

# IT2School

Gemeinsam IT entdecken



## Modul A2 – Kryptologie

### Kryptologie

Eine Entwicklung von



In Kooperation mit



Im Auftrag der



# Inhalt

1	Kryptologie .....	3
2	Warum gibt es das Modul? .....	4
3	Ziele des Moduls.....	4
4	Die Rolle des Unternehmensvertreterin/des Unternehmensvertreters .....	4
5	Inhalte des Moduls.....	4
5.1	Schaubild zur Kryptologie .....	7
5.2	Moderne Kryptologie .....	7
6	Unterrichtliche Umsetzung.....	9
6.1	Datensicherheit im Alltag .....	9
6.2	Grober Unterrichtsplan (exemplarisch).....	10
6.3	Stundenverlaufsskizzen .....	11
7	Einbettung in verschiedene Fächer und Themen .....	14
8	Anschlussthemen.....	15
9	Literatur und Links .....	15
10	Arbeitsmaterialien .....	15
11	Glossar.....	16

# 1 Kryptologie

In diesem Modul befassen sich die Schülerinnen und Schüler mit dem Ver- und Entschlüsseln 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.



<b>Lernfeld/Cluster:</b>	Kommunikation erkunden	
<b>Zielgruppe/Klassenstufe:</b>		4. bis 5. Klasse
	X	6. bis 7. Klasse
	X	8. bis 10. Klasse
	X	11. bis 12. Klasse
<b>Geschätzter Zeitaufwand:</b>	6 Einzelstunden	
<b>Lernziele:</b>	<ul style="list-style-type: none"> <li>• Bedeutung von Verschlüsselung im Alltag und Arbeitswelt kennenlernen</li> <li>• Kryptographische und kryptoanalytische Verfahren kennenlernen</li> <li>• Ausgewählte Verfahren anwenden und „knacken“ können</li> <li>• Eigenen Umgang mit persönlichen Informationen reflektieren und anschließend schützen</li> </ul>	
<b>Vorkenntnisse der Schülerinnen und Schüler:</b>	Keine	
<b>Vorkenntnisse der/des Lehrenden:</b>	Keine	
<b>Vorkenntnisse der Unternehmensvertreterin/des Unternehmensvertreters:</b>	Keine	
<b>Sonstige Voraussetzungen:</b>	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 Wirtschaftsunternehmen 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 Verschlüsselungsvarianten 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**.

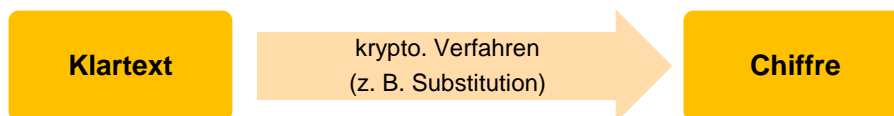
Bei der sogenannten **Transposition** werden Buchstaben oder Wörter im Klartext verschoben, so dass ein Sinnzusammenhang nicht direkt erkennbar wird bzw. der Klartext nicht so leicht lesbar ist. Als ein einfaches historisches Beispiel ist die griechische Skytale zu nennen. Mit Hilfe eines Holzstabes 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 Beispiel 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 Substitutionsverfahrens 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 Chiffrierungszyklindern, 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 Turing die Enigma-Entschlüsselung zu knacken, wodurch sie den Ausgang des 2. Weltkrieges entscheidend beeinflussten.<sup>1</sup>

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 beispielsweise 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.



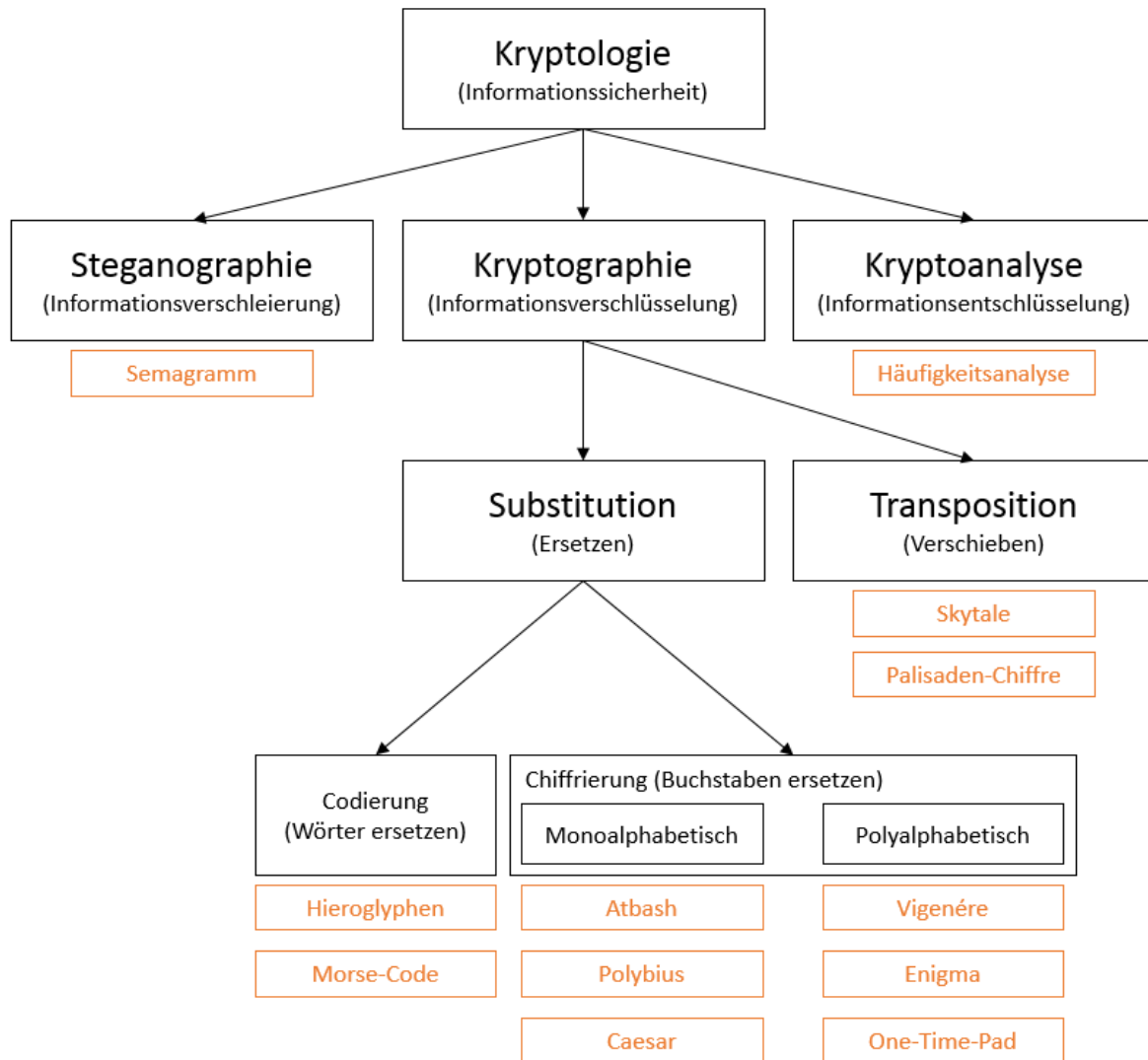
Auch im digitalen Bereich gibt Einsatzgebiete für Semagramme. Innerhalb einer MP3-Audio-Datei oder eines Bildes im JPG-Format lassen sich zusätzliche Bytes einfügen ohne dass sich die ursprüngliche Melodie oder das Bild ändert.

---

<sup>1</sup> 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



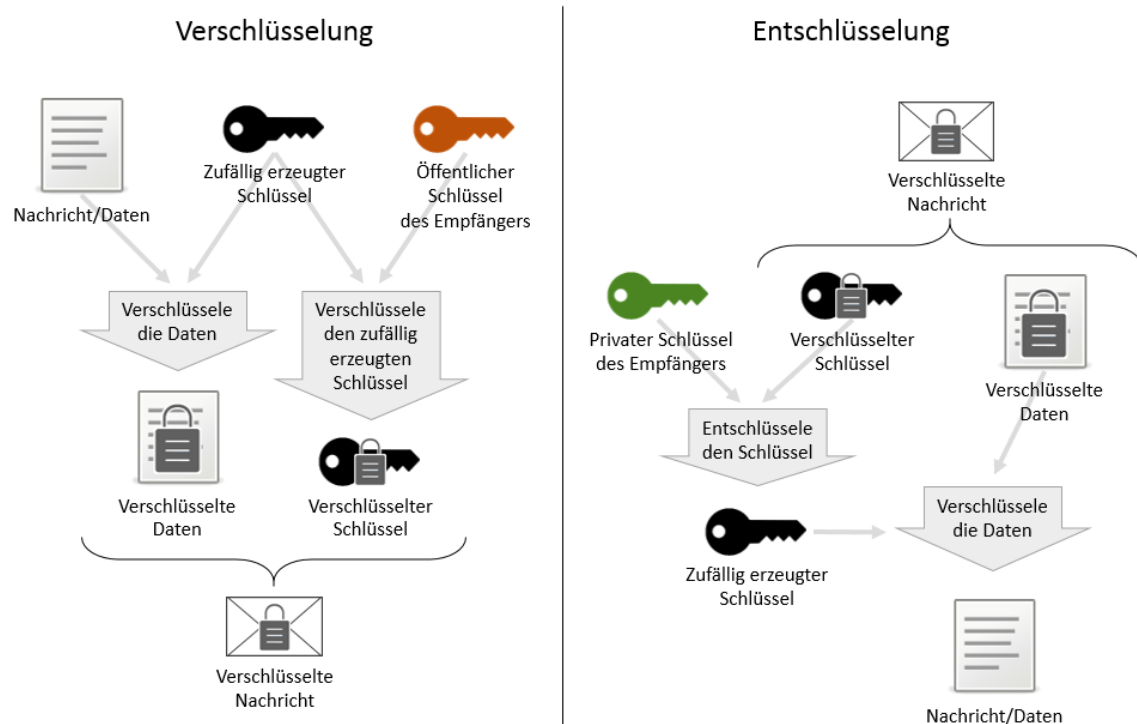
## 5.2 Moderne Kryptologie

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 asymmetrische Verschlüsselung finden in diesem Zusammenhang 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- und Private-Key genannt. Verständlicher wird die asymmetrische 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 Arithmetik. 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 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, die 1991 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 asymmetrischen Verfahren verschlüsselt. Zunächst wird ein zufälliger Schlüssel erzeugt und mit einem asymmetrischen Verfahren verschlüsselt. Dieser zufällige Schlüssel dient zur symmetrischen Verschlüsselung der eigentlich Daten. Das folgende Schaubild zeigt dies etwas genauer:





## 6 Unterrichtliche Umsetzung

Diese Unterrichtseinheit 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 Verschlüsselung 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.	Einstieg	Plenum	Begrüßung der SuS; Erklärung des neuen Themenkomplexes; Aufgabenstellung (MindMap und E-Mail) erklären; Flipchart/ Metaplanpapier verteilen  <i>Frage: Wie kann man die Nachricht entschlüsseln? Gibt es einen Hinweis auf die Verschlüsselung?</i> MindMap: Als einzige Vorgabe wird der Begriff <i>Kryptologie</i> in die Mitte geschrieben.	
25 Min.	Erarbeitung	Einzel-/Partner-/Gruppenarbeit <sup>2</sup>	Die SuS bearbeiten die erste Nachricht und Antworten auf die E-Mail.	
10 Min.	Sicherung	Plenum	Besprechung des Vorgehens und Lösung.	

<sup>2</sup> 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 bisherigen 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, Vigenère ...) 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 Schulbildung 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 kryptographischen Verfahren bzgl. sicherer Kommunikation 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 Anschlusssthemen

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

### Beispiel: Programmieren







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.informatik-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: <ul style="list-style-type: none"> <li>• A wird mit Z verschlüsselt und umgekehrt</li> <li>• B wird mit Y verschlüsselt und umgekehrt</li> <li>• Usw.</li> </ul>
Caesar-Verschlüsselung	Ein monoalphabetisches Substitutionsverfahren, bei dem das Ursprungsalphabet um einen festen Wert verschoben wird. Bei einer Verschiebung von 3 bedeutet dies: <ul style="list-style-type: none"> <li>• A wird mit D verschlüsselt</li> <li>• B wird mit E verschlüsselt</li> <li>• Usw.</li> </ul>
Chiffre	Bezeichnet einen verschlüsselten Text.
Chiffrieren	Bezeichnet das Verschlüsseln eines Klartextes.
Enigma	Bei 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 Ursprungsalphabetes 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 versteckte 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.