Fachdidaktik I
Unterrichtssequenz Einmalverschlüsselung
Jonas Balsiger, Thomas Lehmann und Sergio Mouzo

Verschlüsselung spielt in unserem täglichen Leben oft unbewusst eine wichtige Rolle, sei dies beim E-Banking oder Onlineshopping. Fast überall treffen wir Information an, die geschützt oder verschleiert werden soll: Das reicht von einfachen Passwörtern über Agenden, Daten wie Prüfungen oder Noten aus dem Schulleben, bis zu komplexeren Bauplänen eines Gerätes für Ingenieure oder strategische Firmendaten. Auch könnten (digitale) Tagebücher von Teenagern nur von Auserwählten gelesen (sprich entschlüsselt) werden können. Auch geschichtlich spielte die Kryptographie bzw. -analyse eine grosse Rolle, wenn man sich die strategische Bedeutung der Enigma (Verschlüsselungsmaschine der Wehrmacht) aus der jüngeren Vergangenheit als Beispiel vor Augen führt. Aus anderen Fächern (wie beispielsweise Geschichte oder Deutsch) könnten also bereits Verbindungen auf diesen alltäglichen Wunsch an unsere moderne Technik vorhanden sein.

Unsere Unterrichtsidee wurde für eine Klasse an einem Gymnasium entwickelt, die die Grundkenntnisse der Wahrscheinlichkeitsrechnung aus der Mathematik beherrscht. Im Informatikunterricht wurden bisher Grundkenntnisse zur Kryptographie erlernt, die jetzt gemäss Lehrplan im Teilgebiet zur Sicherheit vertieft werden.

In dieser Einheit bauen wir auf erworbene Fertigkeiten im Bereich der Kryptoanalyse auf und verfeinern diese. Als zeitlichen Rahmen haben wir eine Lektion vorgesehen. Als Sozialform eignen sich besonders die Einzel- oder Gruppenarbeit, um das Lernziel zu vermitteln.

Unser Grundgerüst baut einerseits darauf auf, dass die Klasse das Caesar-Verfahren als Prototyp der monoalphabetischen Verschlüsselung kennengelernt hat und weiss, wie dieses mithilfe einer sprachabhängigen Häufigkeitsanalyse zu knacken ist. Andererseits setzen wir voraus, dass das Vigenère-Verfahren als Prototyp der polyalphabetischen Verschlüsselung bekannt ist und auch, dass der Schlüssel möglichst zufällig und möglichst lang gewählt werden muss, damit beispielsweise der Kasiski-Test nicht greifen kann. Die Wichtigkeit der Einmalschlüssel-Verfahren unterstreicht diese Lektion an einem entwickelten fiktiven Szenario, die es erlaubt, eine Brücke zwischen den erwähnten Verfahren zu schlagen. Einsteigend führen wir mithilfe eines einfachen Rätsels an die Problematik heran und führen durch geschickte Lernaufgaben in die Tiefe des Stoffes. Ein selbst geschriebenes Programm hilft bei der Bearbeitung der Aufgaben und erlaubt den raschen und gezielten, jedoch spielerischen Einsatz der Technik, um die Probleme zu erkennen und zu bewältigen; die Maschine nimmt dabei die mühsame Handarbeit ab und erlaubt so dem Schüler bzw. der Schülerin ein effizientes Auseinandersetzen mit dem Kern der Sache. Dadurch erreicht man das Hauptziel unserer Lektion: Verschiedene Strategien und Verfahren (mit Häufigkeitsverteilungen) aus der Kryptographie gewinnbringend einzusetzen und abzuwägen. Die Überprüfung der Kompetenzen könnte in einer Prüfung beispielweise mit ähnlich gestellten Aufgaben erfolgen. Hierbei eignet sich eine Variation der eingesetzten Schlüssel. Wir könnten uns aber auch vorstellen, interaktiver zu arbeiten, beispielsweise schrittweise die Lösungen der Lehrperson vorzuweisen, die geschickt Hilfestellungen anbieten kann.

Theoretische Sachlage

Die Vigenère-Verschlüsselung ist unter folgenden Bedingungen ein unknackbares Verfahren, wobei alle drei gleichzeitig erfüllt sein müssen:

1. Der Schlüssel besteht aus einer möglichst zufälligen Zeichenfolge.

2. Die Länge des Schlüssels erreicht die des Klartextes.

3. Der Schlüssel wird nicht mehrfach verwendet.

Zu den Bedingungen:

1. Einst wurden lateinische Sinnsprüche als Schlüssel verwendet. Das ist so, als würde man heutzutage zum Beispiel den Songtext eines bekannten Liedes nehmen. Der Schlüssel sollte aber, unabhängig der Länge, auf keinen Fall leicht zu erraten sein.

2. Ist das Verhältnis |Klartext| zu |Schlüsselwort| zu gross, lässt sich unter Umständen mithilfe des Kasiski-Tests die Länge des verwendeten Schlüsselwortes bestimmen und anschliessend mithilfe einer Häufigkeitsanalyse das Schlüsselwort selbst.

3. Heute wird das als One-Time-Pad (DE: „Einmalschlüssel-Verfahren“) bezeichnet. Dabei kann man für jede Nachricht einen Schlüssel der gleichen Länge erzeugen. Sollte sich jedoch ein anhaltendes Gespräch mit demselben Gesprächspartner abzeichnen, so kann man einen überlangen Schlüssel (mehr oder weniger) einmalig sicher austauschen und die jeweiligen Nachrichten so lange damit verschlüsseln, bis der Schlüssel aufgebraucht ist.

Aufgabenstellung / Lösungsstrategien und Zweck der Übung

Aufgabe 1

Sie fangen folgende 10 Kurznachrichten ab, die alle mit dem Vigenère-Verfahren und immer mit demselben Schlüssel der Länge 3 verschlüsselt wurden:

QAE; QWR; QSS; JAE; RAN; MMM; JWR; JWN; QWN; VUH

Hinter jeder der zehn Nachrichten versteckt sich ein deutsches Wort, jeweils der Länge 3. Schaffen Sie es, das Schlüsselwort zu erraten?

Benutzen Sie die folgenden Häufigkeitstabellen für deutschsprachige Texte:

Anfangsbuchstabe

Platz	Buchstabe	Relative Häufigkeit
1.	D	14.2%
2.	S	10.8%
3.	E	7.8%

Ganze Texte

Platz	Buchstabe	Relative Häufigkeit
1.	E	17.4%
2.	N	9.8%
3.	I	7.6%

Lösungsstrategien und Zweck der Übung (Aufgabe 1)

Da alle Nachrichten mit demselben Schlüssel verschlüsselt wurden, sind jeweils alle ersten, alle zweiten und alle dritten Buchstaben, gemäss dem Caesar-Verfahren, um den gleichen Wert im Alphabet verschoben worden. Somit lässt sich spaltenweise eine Häufigkeitsanalyse durchführen.

Als erster Buchstabe taucht «Q» am häufigsten vor. Da «D» der häufigste Anfangsbuchstabe für deutschsprachige Texte ist, liegt die Vermutung nahe, dass hier um 13 Stellen nach rechts verschoben wurde. Das entspricht dem Schlüsselbuchstaben «N».
Als zweiter Buchstabe taucht «W» am häufigsten vor. Die zweite Tabelle lässt vermuten, dass «E» auf «W» abgebildet, das heisst um 18 Stellen nach rechts verschoben wurde. Das entspricht dem Schlüsselbuchstaben «S».

Das Beispiel wurde extra so gewählt, dass das Schlüsselwort tatsächlich mit «NS» beginnt. Da bisher alles auf Wahrscheinlichkeiten und auf Vermutungen basierte, lohnt sich dennoch ein zwischenzeitlicher Blick auf den teilentschlüsselten Text:

DI*;* DE*; DA*; WI*; EI*; ZU*; WE*; WE*; DE*; IC*

Die Bigramme lassen erahnen, dass wir auf dem richtigen Weg sind – und tatsächlich sind die meisten Wörter jetzt bereits erkennbar. Beispielsweise die letzte Geheimnachricht «VUH», die bisher «IC*» lieferte, muss fast zu «ICH» vervollständigt werden. Das entspricht einer Abbildung von «H» auf «H» und somit dem Schlüsselwortendbuchstaben «A».

Alternativ kann man erneut eine Häufigkeitsanalyse auf die jeweils dritten Buchstaben anwenden. Diese Strategie wird dadurch erschwert, dass in diesem Fall ausnahmsweise nicht der statistisch gesehen häufigste Buchstabe «E», sondern der zweithäufigste Buchstabe «N» am stärksten vertreten ist, dicht gefolgt von «E». Würde man «E» auf «N» abbilden wollen, würde man fälschlicherweise den Schlüsselwortbuchstaben «J» und folgende vermeintliche Klartexte erhalten:

DIV; DEI; DAJ; WIV; EIE; ZUD; WEI; WEE; DEE; ICY

Nach einigem Experimentieren würde man sich also auf das Schlüsselwort «NSA» (kurz für «National Security Agency») einigen und folgende Klartexte erhalten:

DIE**;** DER; DAS; WIE; EIN; ZUM; WER; WEN; DEN; ICH

Wir halten fest, dass man selbst das (unknackbare) Vigenère-Verfahren knacken kann, sofern man mehrere Nachrichten abfangen kann, die gleichermassen chiffriert wurden. Dazu muss man nur die Geheimtexte untereinander aufschreiben und spaltenweise, wie beim Caesar-Verfahren, eine Häufigkeitsanalyse darauf anwenden. Hierfür muss man noch nicht einmal die Länge des Schlüssels kennen. So wie beim Kasiski-Test das Verhältnis |Klartext| zu |Schlüsselwort| die kritische Grösse darstellt, ist hier die Anzahl der abgefangenen Nachrichten ausschlaggebend. Die Wichtigkeit der Einmalschlüssel-Verfahren wird uns somit vor Augen geführt.

In Bezug auf die Häufigkeitstabellen ist noch zu beachten, dass es sich stets um relative Häufigkeiten handelt. Ein konkreter Text wird diese kaum exakt annehmen, speziell nicht, wenn er kurz ist. Interessant ist auch zu sehen, dass nicht nur eine Häufigkeitstabelle pro Sprache existiert. Man kann zum Beispiel zwischen Anfangsbuchstaben und Buchstaben allgemein unterscheiden. Aber auch Analysen zu typischen Bigrammen, Trigrammen und Präfixe oder Suffixe von Wörtern können hilfreich sein.

Aufgabe 2

Begründen Sie, weshalb das mehrfache Verwenden desselben Vigenère-Schlüssels das Verfahren unsicher macht, obwohl der Schlüssel gleich lang ist wie der Klartext.

Lösungsstrategien und Zweck der Übung (Aufgabe 2)

Hier gilt es die Erkenntnisse festzuhalten, die man beim Lösen von Aufgabe 1 gewonnen hat.

Aufgabe 3

Würde es etwas bringen, wenn wir den Schlüssel sogar länger als den Klartext selbst wählen?

Lösungsstrategien und Zweck der Übung (Aufgabe 3)

Es wäre nicht hilfreich, wenn man weiterhin jede Nachricht mit demselben Schlüssel verschlüsselt – der hintere Teil des Schlüssels würde einfach ungebraucht bleiben. Das heisst, wir könnten weiterhin alle abgefangenen Nachrichten untereinanderschreiben und wie gehabt spaltenweise eine Häufigkeitsanalyse darauf anwenden.

In diesem Kontext bietet es sich an, die Klasse nochmals darauf hinzuweisen, dass bei symmetrischen Verfahren der sichere Schlüsselaustausch ein Knackpunkt darstellt. Sobald ein solcher aber stattgefunden hat, wäre es demnach eine Verschwendung den Schlüssel, wenn auch nur teilweise, verfallen zu lassen. Um dem entgegenzuwirken, kann man den bereits ausgetauschten Schlüssel so lange verwenden, bis er aufgebraucht ist, um dann wieder von vorne zu beginnen. Das hätte nebenbei den angenehmen Zusatzeffekt, dass man die Nachrichten nicht mehr bedenkenlos untereinanderschreiben könnte, sondern wieder mit dem Kasiski-Test ansetzen müsste, um zunächst die Schlüssellänge herauszufinden.

Aufgabe 4

Nehmen Sie an, die obigen 10 Wörter werden mithilfe der folgenden Tabelle verschlüsselt:

	1	2	3	4	5	6
1	B	O	E	F	R	U
2	H	Q	A	L	N	M
3	I	D	T	K	S	V
4	C	P	G	W	X	Z
5	J	Y				

Hierbei handelt es sich um eine beliebige, rein zufällige Permutation des Alphabets.
Hätten Sie die Geheimbotschaft auch mit dem grundsätzlich schwächeren, monoalphabetischen Verfahren knacken können? Begründen Sie Ihre Antwort.

Lösungsstrategien und Zweck der Übung (Aufgabe 4)

Grundsätzlich lässt sich jedes monoalphabetische Verschlüsselungsverfahren, zumindest im Ansatz, mit einer Häufigkeitsanalyse knacken – dies, obschon es $26!$ (Fakultät) verschiedene Schlüssel gibt. Die abgefangenen Nachrichten werden alle hintereinandergeschrieben und als eine lange Nachricht interpretiert.

Bei 10 Nachrichten mit je 3 Buchstaben ist der Datensatz jedoch nicht besonders aufschlussreich. Der Buchstabe «E» kommt in unserem Beispiel glücklicherweise am häufigsten vor – somit bleiben aber immer noch $25!$ (Fakultät) Möglichkeiten. Doch bereits der statistisch gesehen zweithäufigste Buchstabe «N» teilt sich den vierten Platz mit dem

Buchstaben «W». Hinzu kommt, dass in unserem Beispiel nur 13, also genau die Hälfte aller 26 Buchstaben im Alphabet vorkommen, was eine Analyse zusätzlich erschwert.

Fazit: In unserem Fall ist die ursprünglich unknackbare Vigenère-Verschlüsselung vermutlich sogar einfacher zu knacken als das monoalphabetische Verfahren.
Es gilt jedoch zu beachten, dass die Länge jeder Botschaft und die Anzahl der abgefangenen Nachrichten eine wesentliche Rolle spielen. Fängt man zum Beispiel umgekehrt 3 Nachrichten der Länge 10 ab, so hätte dies zwar keinen Einfluss auf die monoalphabetische Verschlüsselung, die Ausgangslage für die Vigenère-Variante würde sich aber wesentlich verschlechtern.

Aufgabe 5

Sie fangen 50 Nachrichten der maximalen Länge 29 ab, die mit demselben Schlüssel der Länge 29 mit dem Vigenère-Verfahren verschlüsselt wurden. Dabei handelt es sich um zwei unterschiedliche Konversationen mit je zwei Gesprächspartnern in deutscher Sprache. In der Datei ***Geheimtext.txt*** haben Sie alle 50 Nachrichten zeilenweise aufgelistet. Benutzen Sie das Python-Programm ***Main.py***, um das Schlüsselwort zu erraten.
Je mehr Schlüsselbuchstaben man bereits erraten hat, desto einfacher wird es, durch Fragmente von bekannten Wörtern den nächsten Schlüsselbuchstaben ohne Häufigkeitsanalyse zu bestimmen. Dies ist ein weiterer Grund, weshalb ein Vigenère-Schlüssel – und ist er noch so lang – nicht mehrfach verwendet werden sollte.

Lösungsstrategien und Zweck der Übung (Aufgabe 5)

Diese letzte Aufgabe ist teils als Knobelaufgabe, teils als Fleissaufgabe gedacht. Sie soll Gelegenheit bieten, das Gelernte spielerisch anzuwenden und deshalb in erster Linie auch Spass machen.

Wenn man die 50 Zeilen unverschlüsselt liest, kann man zwei unterschiedliche Konversationen mit je zwei Gesprächspartnern in deutscher Sprache verfolgen, die durch die Nachricht «ABCDEFGHIJKLMNOPQRSTUVWXYZ» getrennt sind. Diese «Check-Up-Zeile» sollte in der Praxis natürlich vermieden werden, kann hier aber als Tipp zu gegebenem Zeitpunkt der Klasse mitgegeben werden.

Eine statistische Analyse der jeweils ersten Buchstaben liefert, dass der Buchstabe «R» am häufigsten vorkommt. Unter Zuhilfenahme der ersten Tabelle mit der Häufigkeit der Anfangsbuchstaben nehmen wir an, dass sich ein «D» dahinter verbirgt, was einer Verschiebung um 14 Stellen im Alphabet nach rechts entspricht. Daher vermuten wir den ersten Schlüsselwortbuchstaben «O».
Eine statistische Analyse der jeweils zweiten Buchstaben liefert, dass der Buchstabe «N» am häufigsten vorkommt. Unter Zuhilfenahme der zweiten Tabelle mit der Häufigkeit der Buchstaben allgemein nehmen wir an, dass sich ein «E» dahinter verbirgt, was einer Verschiebung um 13 Stellen im Alphabet nach rechts entspricht. Daher vermuten wir den zweiten Schlüsselwortbuchstaben «N». Und tatsächlich fängt das Schlüsselwort in diesem Beispiel auch mit «ON» an.

In den weiteren Spalten wird der häufigste Buchstabe bewusst nicht mehr immer zwingend dem «E» entsprechen. Zudem sind nicht alle Zeilen 29 Zeichen lang, weshalb eine statistische Analyse in den letzten Spalten etwas weniger gewinnbringend wäre. Ab hier ist es deshalb sinnvoll, wenn man regelmässig einen Blick auf die teilweise dechiffrierte Nachricht wirft und zum Beispiel mithilfe bekannter Präfixe auf die jeweils nächsten Schlüsselwortbuchstaben versucht zu schliessen.

Der Schlüssel lautet dann «*ONETIMEPADISTEINMALSCHLUESSEL*». Natürlich dürfte man in der Praxis keinen Schlüssel verwenden, der leicht zu erraten ist, doch in dieser Aufgabe wollen wir ein Auge zudrücken.

Hinweis für Lehrpersonen *(Backdoor)*

Mithilfe des Programms lässt sich der Schlüssel erstmal nur stellenweise verändern. Als Input wird die Stelle des Buchstabens verlangt, die man anpassen möchte. Gibt man an dieser Stelle nun aber -1 ein, so kann man die ersten n ($\leq$ Schlüssellänge) Buchstaben des Schlüssels in einem Wort eingeben. Dies ist zeitsparend und kann für die Demonstration sinnvoll sein.