Adrian Häfliger GYMINF Fachdidaktik, HS21

Das Public Key Verfahren

Unterrichtseinheit für das Fach Informatik

1 Ziel

- Schüler*innen haben ein Bild, welches Ihnen das grundsätzliche Verständnis für den Einsatz und die Funktionsweise eines Public Key Verfahrens ermöglicht.
- Schüler*innen lernen RSA als ein Public Key Verfahren kennen.
- Schüler*innen erkennen, dass RSA durch eine Kombination von mathematischen Methoden und Erkenntnissen möglich wird.
- Schüler*innen können mit Hilfe eines gegebenen RSA-Programms asymmetrisch einen Schlüssel tauschen und danach Nachrichten symmetrisch ver- und entschlüsseln.

2 Rahmen

2.1 Vorgesehene Zeit

Für die gesamte Einheit sind 2 bis 4 Lektionen vorgesehen, abhängig davon, wie detailliert auf die technischen Aspekte des RSA-Verfahrens eingegangen wird und wie viele praktische Verschlüsselungsübungen die Schüler*innen durchführen sollen.

2.2 Ausgangslage

In den vorangehenden Lektionen wurde das Thema Verschlüsselung allgemein eingeführt und die Schüler*innen haben die symmetrische Verschlüsselung kennengelernt und an Beispielen durchgespielt. Die Schüler*innen haben erkannt, dass der Schlüsseltausch eine Herausforderung für die symmetrische Verschlüsselung darstellt. Zudem wird vor- ausgesetzt, dass die Schüler*innen mit Python vertraut sind und ein gegebenes Programm studieren und über das Terminal anwenden können. Die Einheit kann im Grundlagenfach Informatik im 10. Schuljahr eingesetzt werden und erfordert keine über die im Grundlagenfach Mathematik erworbenen hinausgehenden mathematische Kenntnisse.

2.3 Vertiefung/Anschluss

Als konkrete Anwendung eines Public Key Verfahrens kann mit den Schüler*innen die E-Mail-Verschlüsselung mit PGP behandelt und durchgeführt werden.
Im Anschluss an diese Einheit könnte weiter eine Schwachstelle des Verfahrens herausgearbeitet werden. Gemeint ist die Möglichkeit, dass der versendete öffentliche Schlüssel nicht von der designierten empfangenden Person der Nachricht stammt und die damit von der sendenden Person verschlüsselte Nachricht von der tatsächlich sendenden Person des Schlüssels entschlüsselt werden kann. Dies kann die Überleitung zu einer Behandlung des Themas Authentifizierung sein.

3 Ablauf

3.1 Einstiegsaufgabe (Gruppenarbeit)

Gruppen erhalten ein Fahrradschloss (Schloss mit Schlüssel, welches durch Zusammenstecken auch ohne Schlüssel geschlossen werden kann) und eine Kiste. Der Auftrag lautet: In der Kiste den Schlüssel für eine symmetrische Verschlüsselung sicher transportieren (*Aufgabenblatt 1*). Die Lösung der Aufgabe besteht darin, dass die designierte empfangende Person des symmetrischen Schlüssels zuerst der sendenden Person das geöffnete Schloss schickt, aber den Schlüssel bei sich behält, worauf diese den symmetrischen Schlüssel in die Kiste steckt und diese mit dem Schloss verschliesst und zurückschickt, worauf das Schloss dann von der empfangenden Person mit dem Schlüssel geöffnet werden kann.

3.2 Besprechung der Lösung (Klassengespräch)

Die verschiedenen Lösungsvorschläge werden in der Klasse besprochen. Das Verfahren wird durchgespielt, so dass es für alle Schüler*innen verständlich ist. Die Lehrperson stellt sicher, dass die wesentlichen Aspekte des Verfahrens richtig beschrieben und verstanden sind:

- Die designierte empfangende Person schickt der designierten sendenden Person ein geöffnetes Schnappschloss, zu welchem nur diese den Schlüssel hat; die sendende Person schliesst damit die Kiste ab und schickt die abgeschlossene Kiste an die empfangende Person zurück; die empfangende Person kann die Kiste mit dem Schlüssel öffnen.
- Das geöffnete Schnappschloss kann ohne den Schlüssel abgeschlossen werden, aber nur mit dem Schlüssel geöffnet werden.
- Das geöffnete Schloss kann von allen abgefangen, eingesehen und auch verwendet werden, aber es gibt keinen Weg, um aus dem geöffneten Schloss den Schlüssel zu erhalten.
- Der schlimmste Missbrauchsfall besteht darin, dass jemand anderes als die adressierte Person das Schloss zum verschliessen einer Nachricht verwendet.
- Die designierte empfangende Person der Nachricht muss in einem ersten Schritt das geöffnete Schloss versenden, d.h. die erste Sendung geht von der empfangenden Person aus.
- Es handelt sich um eine asymmetrische Verschlüsselung, bei welcher (im Gegensatz zur symmetrischen Verschlüsselung) unterschiedliche Schlüssel für die Ver- und die Entschlüsselung zur Anwendung kommen.

3.3 Übergang zu RSA (Lehrer*ingespräch)

Nachdem das Verfahren auf bildhafter Ebene verstanden ist, wird eine Brücke zu einer tatsächlichen Umsetzung gebildet. Was sind Schlüssel und Schlösser, welche über elektronische Kanäle versendet werden können? Es wird herausgearbeitet, dass es sich dabei immer nur um Folgen von Symbolen handelt, und zur Frage übergeleitet,

wie damit so etwas realisiert werden könnte? Ausgehend vom Vorgang mit einem physischen Schloss sollen die Merkmale herausgearbeitet werden, welche ein solches Verfahren aufweisen muss:

- Die designierte empfangende Person verschickt der desgnierten sendenden Person eine Folge von Symbolen, welche wie ein geöffnetes Schnappschloss funktioniert: Damit kann eine Nachricht verschlüsselt werden, welche ohne den Besitz des Schlüssels nicht wieder entschlüsselt werden kann.
- Die designierte empfangende Person hat eine zusätzliche Information, mit welcher die Nachricht entschlüsselt werden kann.
- Aus der Information, welche der sendenden Person zugeschickt wurde und von welcher angenommen werden muss, dass sie auch für andere zugänglich ist, kann nicht auf die Information geschlossen werden, welche für das Entschlüsseln benötigt wird.

3.4 Einführung RSA (Lehrer*invortrag)

Ausgehend von den herausgearbeiteten abstrakten Anforderungen an ein Public Key Verfahren wird in Grundzügen die RSA- Verschlüsselung erklärt, wobei die eingeführten mathematischen Verfahren immer deutlich in Bezug zum Bild mit dem Schnappschlossverfahren gesetzt werden:

- Der Schlüssel ist ein Paar von sehr grossen Primzahlen p und q, das geöffnete Schloss ist das Produkt n dieser Primzahlen.
- n dient als geöffnetes Schloss, welches verschickt werden kann und zur Verschlüsselung einer Nachricht dient. Entschlüsselt kann diese Nachricht nur mit Hilfe von p und q werden, weshalb diese beiden Zahlen auch Geheimzahlen genannt werden.
- Es kann einfach beschrieben werden, wie man von der bekannten Zahl n auf die Geheimzahlen kommt: Es müssen einfach die zwei Zahlen gefunden werden, deren Produkt n ist. Dazu kann ein einfacher Algorithmus beschrieben werden: Beginnend bei 2 wird jede Zahl kleiner als $n-1$ durch n dividiert, wenn dies ohne Rest geht, sind die beiden Faktoren gefunden. Dies kann sogar noch optimiert werden, da die Faktoren maximal $\sqrt{n}$ gross sein können. Aber für grosse Zahlen sind das sehr viele Zahlen, die ausprobiert werden müssten.
- Für sehr grosse Zahlen (was bei n der Fall ist) ist es deshalb praktisch unmöglich aus der Kenntnis von n auf p und q zu schliessen. *Praktisch unmöglich* bedeutet hier: Theoretisch ist dies sehr einfach möglich, weil ein einfacher Algorithmus beschrieben werden kann - aber auch der beste bekannte Computer würde mehrere Milliarden Jahre benötigen, um den besten bekannten Faktorisierungsalgorithmus auszuführen.
- Das geöffnete Schloss kann mit einer Verschlüsselungs-Rechnung geschlossen werden:

$$nachricht^{65537} \bmod n = chiffre$$

Das Resultat dieser Rechnung ist die verschlüsselte Chiffre. Diese Rechnung ist normalerweise unumkehrbar: Wenn $chiffre$ und n bekannt sind, kann $nachricht$ nicht berechnet werden. Diese Unumkehrbarkeit liegt in der Modulorechnung begründet. Das Durchführen der Verschlüsselungs-Rechnung entspricht dem Schliessen eines geöffneten Schlosses.

- Im speziellen Fall, wo n das Produkt aus zwei Primzahlen ist und diese beiden Primzahlen bekannt sind, gibt es eine Möglichkeit, die Rechnung umzukehren und aus der $chiffre$, p und q auf die $nachricht$ zu kommen. Dazu muss nach einem bestimmten Verfahren aus p und q eine Zahl d bestimmt werden, worauf die folgende Entschlüsselungs-Rechnung das gewünschte Resultat liefert:

$$chiffre^d \mod n = nachricht$$

  Das Durchführen der Entschlüsselungs-Rechnung entspricht dem Öffnen des Schlosses mit dem Schlüssel. Dieser Vorgang kann nur mit Hilfe der Geheimzahlen p und q durchgeführt werden.

- Diese Möglichkeit verdanken wir einem Satz aus der Zahlentheorie, welcher der Baseler Mathematiker Leonhard Euler (1707 - 1783) entdeckt und bewiesen hat. Ronald L. Rivest, Adi Shamir und Leonard Adleman haben entdeckt, wie dieser Satz für ein asymmetrisches Verschlüsselungsverfahren verwendet werden kann und dies 1977 öffentlich beschrieben. Bis heute wird das Verfahren sehr verbreitet eingesetzt.

- Die empfangende Person verschickt also die Zahl n als geöffnetes Schloss an die sendende Person, die sendende Person führt mit ihrer Nachricht und n die Verschlüsselungs-Rechnung aus und schickt die erhaltene Chiffre an die empfangende Person. Die empfangende Person kann mit Hilfe von p und q die Entschlüsselungs-Rechnung durchführen und erhält die ursprüngliche Nachricht.

- Da die Verschlüsselungs-Rechnung im Normalfall unumkehrbar ist, funktioniert dies wie ein geöffnetes Schnappschloss: Man kann es ohne den Schlüssel schliessen. In diesem speziellen Fall gibt es eine Umkehrmöglichkeit, aber nur, wenn die beiden Primzahlen bekannt sind - das heisst, es gibt einen Schlüssel, mit dem das geschlossene Schloss wieder geöffnet werden kann. Die beiden Primzahlen können praktisch nicht aus der verschickten Zahl berechnet werden - das heisst, aus dem offen versendeten Schloss kann der Schlüssel nicht eruiert werden. Nur wer die beiden Primzahlen besitzt, kann die Entschlüsselungs-Rechnung durchführen - das heisst, nur wer den Schlüssel besitzt, kann das geschlossene Schloss wieder öffnen.

- Die Sicherheit des Verfahrens hängt einzig davon ab, dass die Geheimzahlen wirklich geheim sind. Daraus folgt einerseits, dass es wichtig ist, mit diesen sorgfältig umzugehen. Und zweitens folgt daraus, dass das Verfahren sofort seine Sicherheit verliert, sollte ein Verfahren entwickelt werden, welches in brauchbarer Zeit die Faktoren auch einer sehr grossen Zahl bestimmen könnte. Für Quantencomputer gibt es tatsächlich einen solchen Algorithmus, aber bis heute gibt es noch keine funktionierenden Quantencomputer und viele Experten gehen davon aus, dass es auch in absehbarer Zukunft keine solche geben wird.

3.5 Studieren/Anwenden des RSA-Programms (Einzelarbeit)

Die Schüler*innen erhalten das Programm RSA.py und den Auftrag, dieses zu studieren und auszuprobieren (*Aufgabenblatt 2*).

3.6 Anwenden von RSA (Gruppenarbeit)

In 3-er Gruppen wenden die Schüler*innen das RSA-Verfahren zum verschlüsselten Austausch eines symmetrischen Schlüssels und zur anschliessenden Verschlüsselung an (*Aufgabenblatt 3*).

4 Fachdidaktische Überlegungen

Die **Einstiegsaufgabe** soll das Bewusstsein für eine der Problemstellungen wecken, welche die Entwicklung des Public Key Verfahrens motivierte. Die Aufgabenstellung soll so sein, dass ein grosser Teil der Schüler*innen die Aufgabe lösen kann und alle ein einprägsames Bild für das Public Key Verfahren haben: Die designierte empfangende Person der Nachricht schickt der designierten sendenden Person ein geöffnetes Schnappschloss, mit welchem jene ihre Nachricht sichert. Die von den Gruppen zu erbringende Hauptleistung besteht in der Idee, den Schlüssel vom Schloss zu trennen und das geöffnete Schloss alleine zu versenden, so dass es mit der Schnappfunktion geschlossen werden kann. Um den Lernprozess möglichst nachhaltig zu machen, steckt der Schlüssel am Anfang im Schloss und die Schnappfunktion wird nicht erwähnt.
Das eigentliche Ziel der Aufgabe ist bewusst das Versenden von symmetrisch verschlüsselten Nachrichten, damit bei den Schüler*innen das Verständnis für eine wesentliche Aufgabe des Public Key Verfahrens - den Schlüsseltausch - gezielt gefördert wird. Dies ist zwar nicht der einzige Einsatz von RSA, so kann RSA als eigenständiges Kryptosystem zum direkten Austausch von Nachrichten verwendet werden, zudem wird sehr verbreitet zur Authentifizierung verwendet (z.Bsp. von Websiten). Da aber für symmetrische Verschlüsselungen sehr effiziente technische Verfahren existieren, wird die vergleichsweise aufwendige asymmetrische Verschlüsselung mit RSA in der Praxis oftmals nur für den Schlüsseltausch verwendet. Dies kann im Klassengespräch von der Lehrperson erwähnt werden. Im Aufgabenblatt wird ein 8-stelliger Schlüssel zur Verschlüsselung einer 8-stelligen Nachricht verwendet, bei der der Buchstabe an jeder Stelle um die angegebene Anzahl verschoben wird. Das Verfahren wurde entweder genauso in der vorhergegangenen Einheit zur symmetrischen Verschlüsselung angewendet oder es wird mit der Aufgabenstellung kurz erklärt. Es wurde ein Verfahren gewählt, dass die Mindestanforderungen an eine symmetrische Verschlüsselung erfüllt. Um die Konzentration nicht auf die symmetrische Verschlüsselung zu lenken, sollte es jedoch so einfach wie möglich sein. Zudem sollte der Schlüssel eine Zahl sein, damit dieser bei der späteren Anwendung im RSA-Verfahren nicht zuerst in eine Zahl umgewandelt werden muss.
Alternativ könnte mit Zahlenschlössern gearbeitet werden, welche geschlossen werden können, ohne dass der Code eingestellt ist und bei welchen der Code frei wählbar ist. Dies ergäbe die Möglichkeit, mehrere Schlösser mit demselben Code zu versehen und an mehrere Adressaten zu versenden. Dadurch könnte veranschaulicht werden, dass im Public Key Verfahren der öffentliche Schlüssel an mehrere Parteien versendet werden kann. Allerdings meine ich, dass ein Schloss mit einem Schlüssel, welcher vom

Schloss getrennt werden kann, das einprägsamere Bild für das Verfahren ergibt.
In der anschliessenden **Besprechung** können im Vergleich mit alternativen Bildern die Merkmale des Verfahrens weiter herausgearbeitet werden: Ein geöffnetes Zahlenschloss könnte die Aufgabe nicht erfüllen, weil der Schlüssel abgelesen werden kann; ein Schloss, welches über keine Schnappfunktion verfügt, kann die Aufgabe ebenfalls nicht erfüllen. Bei der versendeten Nachricht handelt es sich um einen symmetrischen Schlüssel, dieser wird im Anschluss an den Tausch zur Ver- und Entschlüsselung von weiteren Nachrichten verwendet. Damit soll für die Schüler*innen verständlich werden, was die hauptsächliche Aufgabe des Public Key Verfahrens ist, nämlich der Austausch eines Schlüssels für die symmetrische Verschlüsselung. Es kann auch thematisiert werden, was passiert, wenn das geöffnete Schloss von anderen abgefangen und verwendet wird: Sie können damit ebenfalls etwas abschliessen, was nur von der Besitzerin des Schlüssels wieder geöffnet werden kann - sie können aber keine mit diesem Schloss verschlossenen Kisten öffnen. Der Begriff der asymmetrischen Verschlüsselung wird anhand des Beispiels herausgearbeitet und mit jenem der symmetrischen Verschlüsselung kontrastriert.
Zum Abschluss der Besprechung der Einstiegsaufgabe wird eine **Brücke zum RSA-Verfahren** gebildet. Die Lehrperson stellt den Bezug zum elektronischen Versenden von Nachrichten her und erläutert, dass ein ähnliches Verfahren für die Verschlüsselung elektronischer Nachrichten wichtig wäre. Das RSA-Verfahren selbst kann selbstverständlich nicht im entwickelnden Klassengespräch eingeführt werden, aber in einem solchen Gespräch können ausgehend vom Schloss-Verfahren die abstrakten Anforderungen an ein solches Verfahren herausgearbeitet und so allgemein beschrieben, dass die später eingeführte Umsetzung im RSA-Verfahren daran gemessen werden kann.
Im Lehrer*invortrag zur **Einführung von RSA** werden die wichtigsten Aspekte des Verfahrens eingeführt und erläutert. Der Fokus liegt dabei auf dem grundsätzlichen Verfahren und jenen Aspekten, welche zuvor am Schlossbeispiel herausgearbeitet wurden. Die Unumkehrbarkeit der Modulorechnung wird als Schnappfunktion beschrieben, die praktische Nicht-Faktorisierbarkeit grosser Zahlen als Unmöglichkeit, aus dem geöffneten Schloss den Schlüssel zu eruieren. Die Schwierigkeit des Faktorisierens kann exemplarisch an einigen Beispielen aufgezeigt werden. Je nach zur Verfügung stehender Zeit und mathematischen Interessen der Klasse können die mathematischen Hintergründe vertieft werden; es ist aber gut vorstellbar, dass das Verfahren dargestellt wird, ohne beispielsweise genauer auf die Modulorechnung einzugehen.
Speziell betont werden kann im Lehrervortrag, dass das ganze Verfahren auf einer Entdeckung aus dem 18. Jahrhundert, deren praktischer Nutzen während fast 300 Jahren nicht gesehen werden konnte, basiert. Daran kann gezeigt werden, dass der Nutzen von Forschung nicht immer konkret sichtbar ist, dass es aber dennoch wichtig ist, in Grundlagenforschung zu investieren. Diese Idee kann noch weiter geführt werden: Ein Bereich, in welchem heute Grundlagenforschung betrieben wird, sind Quantencomputer. Und vielleicht sind es irgendwann die Ergebnisse dieser Grundlagenforschung (oder einer anderen Grundlagenforschung, welche wir uns im Moment gar nicht vorstellen können), welche das RSA-Verfahren zum Einstürzen bringen wird.
Da das Lernziel nicht darin besteht, die exakte Funktionsweise eines Public Key Verfahrens zu verstehen, sondern das grundsätzliche Prinzip und seine Anwendung, wird den Schüler*innen ein Python-Programm abgegeben zum **Studieren und Anwenden von RSA**. Mit dem Programm können Schlüssel generiert und Nachrichten ver-

und entschlüsselt werden. Das Programm ist darauf angelegt, dass seine Nutzung die wesentlichen Grundzüge von RSA erfahrbar macht. Im Vergleich zur gängigen Terminologie und Handhabung wurden deshalb Änderungen vorgenommen. Der öffentliche Schlüssel ist beim RSA-Verfahren ein Paar von Zahlen (e, n), wobei n das Produkt der beiden grossen Primzahlen für den privaten Schlüssel und e der gewählte Exponent für die Verschlüsselung (teilerfremd zu $\phi(n)$) ist. Um den Fokus auf n zu richten, ist e beim Programm fix als 65537 eingestellt, es handelt sich dabei um die Zahl, welche in vielen tatsächlichen Anwendungen verwendet wird. Der private Schlüssel ist im herkömmlichen Verfahren ein Paar von Zahlen (d, n), wobei d aus den beiden grossen Primzahlen und e generiert wird und n das Produkt der beiden Primzahlen ist. Um den Fokus auf die beiden Primzahlen zu richten, werden die beiden Primzahlen als privater Schlüssel verwendet. Das Programm generiert daraus d und n, welche dann zur Entschlüsselung verwendet werden.
Abgesehen von diesen Vereinfachungen soll das Programm jedoch so realistisch wie möglich sein: Wenn die Schüler*innen mit Hilfe dieses Programms Nachrichten verschlüsseln, so entspricht deren Sicherheit den modernsten Standards. So werden Primzahlen in einer realistischen Grösse verwendet, so dass die Schüler*innen ein Gefühl für deren Grösse erhalten und erfahren, dass es vergleichsweise lange dauert, solche Zahlen zu generieren. Zudem soll die Anwendung des Programms dazu führen, dass die Schüler*innen gut zwischen den drei im Verfahren beteiligten Zahlen unterscheiden können und sich auch Gedanken dazu machen müssen, wie diese Zahlen gespeichert und geteilt werden können.
Alle Methoden und Programmteile sind ausführlich kommentiert. Die Kommentare haben den Anspruch, das RSA-Verfahren möglichst korrekt und detailliert zu erklären und aufzuzeigen, wie das vorliegende Programm dieses umsetzt. Das Ziel ist es nicht, dass alle Schüler*innen alle Erläuterungen im Detail nachvollziehen können, aber dass sie verstehen, dass es möglich ist, diese im Detail nachzuvollziehen. Zur Binnendifferenzierung kann der Grad, in welchem das Verfahren von den Schüler*innen nachvollzogen wird, erhöht werden. Entscheidend ist die Einsicht, dass es sich um ein öffentlich bekanntes Verfahren handelt, was dadurch deutlich wird, dass dasselbe Programm zum Verschlüsseln und Entschlüsseln verwendet wird, dass aber die Kenntnis des durch das Programm implementierten Verfahrens nicht genügt, um eine Nachricht zu entschlüsseln.
Die zweite Aufgabe bereitet die anschliessende Gruppenaufgabe vor, indem die Schüler*innen aufgefordert werden, das gesamte Verfahren schematisch darzustellen und somit einen Überblick über die einzelnen Bestandteile zu gewinnen.
Die abschliessende **Anwendungsaufgabe zum RSA-Verfahren** hat zum Ziel, dass die Schüler*innen den gesamten Vorgang des Schlüsseltauschs mit dem RSA-Verfahren und dem anschliessenden Austausch von symmetrisch verschlüsselten Nachrichten durchspielen und so das mit dem Schloss und der Kiste erprobte Verfahren auch in einer technischen Umsetzung anwenden können. Bewusst wird die Aufgabenstellung als eine grosse Aufgabe formuliert und nicht in die einzelnen Teilprozesse zerlegt. Die Teilprozesse zu erkennen und in der richtigen Reihenfolge von den richtigen Akteur*innen auszuführen, ist die zu erbringende Hauptleistung bei dieser Aufgabe. Es wird vorgegeben, dass die Nachrichten in einem Chat ausgetauscht werden, so dass die angreifende Person die Nachrichten auch mitlesen kann. Dadurch sollte für sie deutlich werden, dass sie grundsätzlich damit rechnen müssen, dass Nachrichten auch von nicht adressierten Akteur*innen gelesen werden können und Verschlüsselung de-

shalb wichtig ist. Dass es mit Hilfe eines Public Key Verfahrens möglich ist, auch unter solchen Voraussetzungen einen gesicherten Schlüsseltausch vorzunehmen, sollte bei den Schüler*innen als grosse Errungenschaft erkannt werden. Beim Durchführen stellen sich konkrete Probleme, zu welchen eine Lösung gefunden werden muss, beispielsweise müssen sie sich überlegen, wo und in welcher Form sie die Geheimzahlen speichern. Im Gespräch mit den Gruppen kann die Lehrperson über diese Frage diskutieren. Die gestellte Diskussionsaufgabe soll dazu anregen, Schwächen des Verfahrens zu suchen - es bietet sich an, diese Diskussion zum Abschluss der Sequenz im Klassenverband aufzunehmen.