Asymmetrische Kryptographie für die Sek I
RSA (fast) ohne Mathematik?

Helmut Witten Brandenburgische Str. 23 10707 Berlin ***helmut@witten-berlin.de***	Bernhard Esslinger Universität Siegen Institut für Wirtschaftsinformatik 57068 Siegen ***esslinger@fb5.uni-siegen.de***
Andreas Gramm Fachseminar für Informatik Menzel-Schule (Gymn.) Altonaer Str. 26 10555 Berlin ***gramm@menzelschule.de***	Malte Hornung Freie Universität Berlin Fachbereich Mathematik und Informatik Didaktik der Informatik 14195 Berlin ***malte.hornung@fu-berlin.de***

Abstract: Angesichts der häufigen Nutzung der elektronischen Kommunikationsmittel wie E-Mail auch durch Jugendliche sowie der weitverbreiteten Unkenntnis hinsichtlich der Risiken einer solchen Kommunikation bedarf es einer Grundbildung in Fragen der Computersicherheit, die über das Verständnis und ggf. die Programmierung des Caesar-Verfahrens hinausgeht. Mit unserer Unterrichtsreihe wollen wir einen u. E. wichtigen Baustein zum Verständnis der asymmetrischen Kryptographie liefern, der schon in der Sekundarstufe I erarbeitet werden kann und somit potenziell allen Schülerinnen und Schülern zur Verfügung steht. Eine ausführlichere und mathematisch-informatisch fundiertere Behandlung des RSA-Verfahrens wird nach wie vor erst in der Oberstufe möglich sein.

1 Warum asymmetrische Kryptographie?

In der Unterrichtsreihe „E-Mail (nur?) für Dich“[1] wird das Thema Verschlüsselung im Kontext der „elektronischen Post“ behandelt. Die aktuelle JIM-Studie[2] zeigt, dass auch im Zeitalter von SchülerVZ, Twitter und Facebook dieser Kommunkationsweg sehr häufig genutzt wird. Dies trifft nicht nur für Jugendliche zu, auch bei technikferneren

[1] s. http://www.informatik-im-kontext.de => Entwürfe

[2] Medienpädagogischer Forschungsverband Südwest, JIM-Studie 2010: Jugend, Informatik, (Multi-Media), Stuttgart 2010. http://www.mpfs.de/fileadmin/JIM-pdf10/JIM2010.pdf

Erwachsenen nimmt nach unseren Erfahrungen die Zahl der „E-Mail-Verweigerer“ langsam, aber stetig ab. Wie man eine E-Mail schreibt, weiß mittlerweile also (fast) jeder Jugendliche. Welche informationstechnischen Systeme sich dahinter verbergen und welche Unsicherheiten elektronische Kommunikation mit sich bringt, bleibt dabei den meisten verborgen. Die Unterrichtseinheit „E-Mail (nur) für Dich“ hat sich zum Ziel gesetzt, die technischen Strukturen vom System E-Mail aufzuzeigen, um Schülerinnen und Schülern einen bewussten und sicheren Umgang mit dem Medium zu ermöglichen.

Im ersten Lernabschnitt wird in die technischen Grundlagen des E-Mail-Dienstes eingeführt. Zentral ist dabei der Begriff Protokoll. Darüber hinaus werden Möglichkeiten der Manipulation von E-Mails aufgezeigt. Damit wird versucht, die Lernenden für die Frage zu sensibilisieren, wie man bei der E-Mail-Kommunikation Sicherheit und Vertraulichkeit herstellen kann. Die Antwort auf diese Frage liegt nahe: Verschlüsselung!

Da die Kryptologie ein umfangreiches Gebiet ist, wird den Schülerinnen und Schülern ein Pfad vorgegeben, auf dem sie das Thema durchschreiten können: Ausgehend von unsicheren symmetrischen Verschlüsselungsverfahren führt der Weg über ein beweisbar sicheres Verfahren – dem „One-Time-Pad“ (siehe unten) – hin zu RSA.

Einfache Substitutionsverfahren wie die Caesar-Chiffre arbeiten mit der Verschiebung von kompletten Alphabeten, ohne die Reihenfolge der Zeichen zu variieren. So lässt sich eine mit Caesar verschlüsselte Nachricht in 25 Versuchen durch systematisches Ausprobieren auch ohne Kenntnis des Schlüssels knacken.

Werden die Zeichen des Geheimtextalphabets jedoch in beliebiger Reihenfolge arrangiert, so erhöht sich die Anzahl möglicher Zuordnungen erheblich:

26! = 403.291.461.126.605.635.584.000.000 (403.291 Trilliarden).

Bei dieser astronomisch hohen Anzahl ist ein systematisches Ausprobieren aller Schlüssel auch mit moderner Computertechnik nicht mehr möglich. Bei Verfügbarkeit längerer Textpassagen lässt sich die Verschlüsselung jedoch auf Grundlage einer Häufigkeitsanalyse knacken (vgl. z. B. die Geschichte „Der Goldkäfer“ von E. A. Poe).

Diese Erkenntnis hat zur Entwicklung polyalphabetischer Verfahren wie z. B. dem Vigenère-Verfahren geführt. Hierbei wird bei jedem Buchstaben das Caesar-Verfahren mit einem anderen Schlüsselbuchstaben angewendet, es handelt sich sozusagen um ein „Multi-Caesar-Verfahren“. Die wechselnden Schlüsselbuchstaben werden in einem Schlüsselwort zusammengefasst. Sind die Schlüsselwörter mindestens so lang wie der Klartext, zufällig gewählt und werden nur einmalig verwendet (Prinzip One-Time-Pad), so garantiert das Verfahren 100%ige Sicherheit. Verstöße gegen diese Voraussetzungen können dann aber trotzdem eine Entschlüsselung ermöglichen. So führte etwa das Projekt VENONA aufgrund fehlerhafter One-Time-Pad-Verschlüsselung zur Enttarnung mehrerer in den USA aktiver sowjetischer Atomspione.[3]

[3] http://de.wikipedia.org/wiki/VENONA-Projekt

Aufbewahrung und Transport der geheimen Schlüsselwörter stellte aber selbst für Geheimdienste im 20. Jahrhundert eine große Herausforderung dar. In Zeiten des Internet mit milliardenfachem Nachrichtenaustausch wird dies zur Unmöglichkeit. Mit der asymmetrischen Kryptographie wurden in der zweiten Hälfte des 20. Jahrhunderts Verfahren entwickelt, die ohne den vorherigen Austausch geheimer Schlüssel auskommen. Das bekannteste Verfahren (RSA) wird heute in vielen Web-Sicherheits-Technologien wie SSL/TLS benutzt, um Sitzungsschlüssel für eine (schnellere) symmetrische Verschlüsselung auf sicherem Wege auszutauschen.

2 Asymmetrische Kryptographie

Somit kann den Lernenden die Existenz sicherer symmetrischer Verschlüsselungsverfahren relativ einfach plausibel gemacht werden, auch wenn die in der Internet-Kommunikation tatsächlich verwendeten Verfahren (DES, IDEA) aus Zeitgründen nicht besprochen werden. Damit ist aber das Problem sicherer Kommunikation über das Internet noch keineswegs gelöst. Zentral dabei sind die Möglichkeiten, die die asymmetrische Kryptographie für den sicheren Schlüsselaustausch und die Authentifizierung der Nutzer bietet. In den meisten Fällen wird dazu das RSA-Verfahren verwendet. Zum Verständnis dieses Verfahrens wird etwas elementare Zahlentheorie benötigt, die unseren Lernenden in der Sekundarstufe I leider nicht zur Verfügung steht. Für die Unterrichtseinheit haben wir daher nach Möglichkeiten gesucht, das Prinzip der RSA-Verschlüsselung mit einem Minimum von Mathematik zumindest plausibel zu machen. Das zentrale Mittel dafür ist die RSA-Demo aus dem vielfach ausgezeichneten CrypTool-Programmsystem (s. http://www.cryptool.de/). Weitere Anregungen erhielten wir aus der von Bernhard Esslinger erstellten Schritt-für-Schritt-Anleitung „Asymmetrische Kryptologie“, die allerdings in ihrer Gesamtheit zu umfangreich für unser Unterrichtsvorhaben war. [4]

[4] Siehe https://www.cryptoportal.de => Unterrichtsmaterial bzw. https://www.cryptoportal.org/data/Asymmetrische%20Kryptologie%20am%20Beispiel%20RSA%20entdecken_v1.1.pdf

2.1 Trennung von Ver- und Entschlüsselung mittels Falltürfunktion

Grundlegend für die asymmetrische Kryptographie sind Einwegfunktionen mit Falltür. Einwegfunktionen sind dadurch charakterisiert, dass sie leicht berechenbar sind, ihre Umkehrfunktion aber nur mit riesigem Rechenaufwand bestimmt werden kann. Bei einer Einwegfunktion mit Falltür (kurz: Falltürfunktion) gibt es eine „Hintertür“, mit deren Kenntnis die Umkehrfunktion wiederum leicht zu bestimmen ist. Ein Beispiel dafür ist ein Briefkasten: Während das Einwerfen eines Briefes einfach ist, ist es schwer, ihn danach wieder herauszufischen – es sei denn, man hat den Schlüssel zum Briefkasten. Im Unterricht werden Vorhängeschlösser als ein Beispiel für eine Falltürfunktion eingesetzt. Auch hier ist es einfach, ein Schloss durch Zudrücken zu schließen, das Schloss ohne Schlüssel zu öffnen ist allerdings aufwändig. Mit diesem Hilfsmittel entdecken die Lernenden den Diffie-Hellman-Schlüsseltausch. Eine ausführliche Beschreibung dieses Einstiegs in die asymmetrische Kommunikation findet sich in den Materialien (s. http://www.informatik-im-kontext.de => „E-Mail (nur?) für dich“).

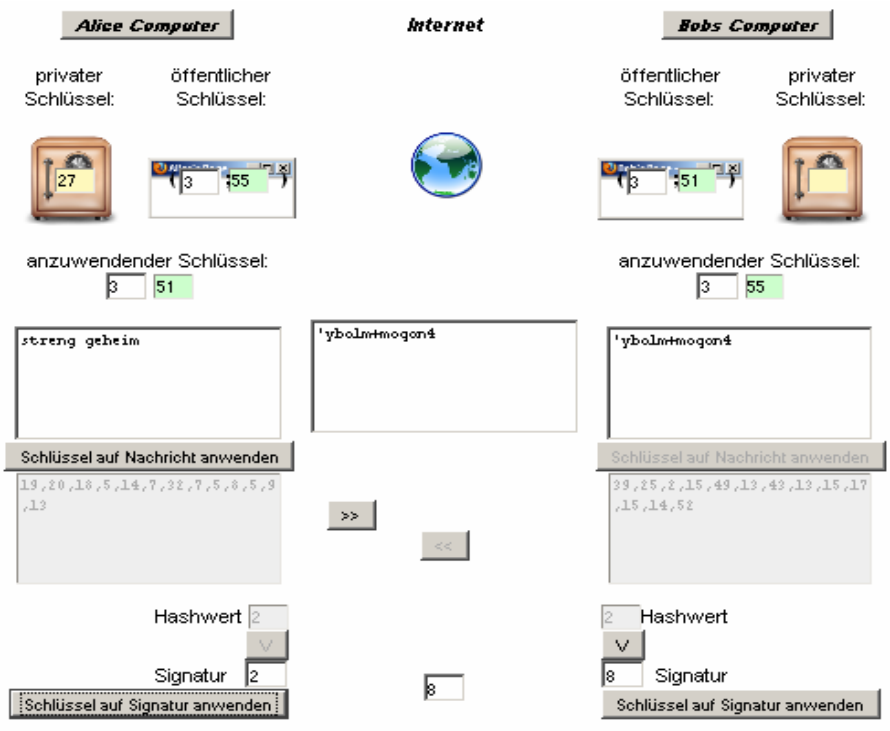

Abb. 1: Animation zur Erarbeitung des Prinzips der asymmetrischen Kryptographie

Die Schülerinnen und Schüler erarbeiten sich dann mit der Animation „Vertraulichkeit und Authentizität durch asymmetrische Kryptologie herstellen“ das Prinzip der asymmetrischen Kryptographie im E-Mail-Kontext[5] (s. Abb. 1). Dabei lernen sie die Funktion von öffentlichen und privaten Schlüsseln kennen. In der Animation wird der geheime Schlüssel durch einen kleinen Tresor symbolisiert: Der Inhalt von Alice‘ Tresor ist immer nur für denjenigen sichtbar, der gerade die Rolle von Alice einnimmt (und entsprechend für Bob). Der öffentliche Schlüssel wird durch eine kleine Webseite dargestellt. Die Weltkugel dazwischen soll einerseits verdeutlichen, dass die öffentlichen Schlüssel weltweit einsehbar sind. Außerdem geht es bei E-Mail um weltweite Kommunikation, auch das soll durch die Weltkugel angedeutet werden.

Hiermit wird die Grundlage für die Beschäftigung mit RSA gelegt, während der eigentliche Verschlüsselungsvorgang hier noch als „Black-Box“ funktioniert. Außerdem ist zu beachten, dass die verwendeten Schlüssel für eine sichere Kommunikation viel zu klein sind, Informationen über die erforderlichen Schlüsselgrößen erhalten die Lernenden im weiteren Verlauf der Unterrichtsreihe.

2.2 Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und Zerlegung in Primfaktoren

In den vorangegangenen Stunden haben die Schülerinnen und Schüler bereits ein physisches Beispiel für eine Falltürfunktion kennen gelernt: das Vorhängeschloss. Für die asymmetrische Verschlüsselung ist aber eine andere Falltürfunktion von Interesse: die Primzahlfaktorisierung: Es ist zwar einfach, das Produkt aus Primzahlen zu erzeugen; die Zerlegung großer Zahlen in ihre Primfaktoren ist jedoch – je nach Größe der Zahl – schwierig bis unmöglich. Eben diese Tatsache macht sich die asymmetrische Verschlüsselung mit dem RSA-Kryptosystem zu Nutze: Während ich aus ausschließlich mir bekannten Primzahlen ohne Schwierigkeiten ein Produkt erzeugen und veröffentlichen kann (öffentlicher Schlüssel), so ist es mit heutiger Rechentechnik bei den z. Zt. üblichen Schlüsselgrößen (mind. 1024 Bit) unmöglich, aus diesem Produkt auf die Primfaktoren zu schließen. Solche Produkte aus genau zwei verschiedenen Primzahlen werden Semiprimzahlen genannt.

Schon bald gelten 1024-Bit-Verschlüsselungen als nicht mehr sicher. Man nimmt an, dass man mindestens 2048-Bit-lange Semiprimzahlen braucht, damit die RSA-Verschlüsselung für viele Jahre ausreichende Sicherheit bietet – mit zunehmender Rechenleistung und der Weiterentwicklung der mathematischen Methoden steigt auch der Aufwand, den man bei der Verschlüsselung betreiben muss. Sollte ein revolutionär neues und effizientes Verfahrens zur Primzahlfaktorisierung erfunden werden, würde aber auch

[5] Der Arbeitsbogen steht unter http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/Animationen%20asymmetrische%20Kryptographie/Integritaet%20und%20Authentizitaet%20mit%20digitaler%20Unterschrift%20sicherstellen.html online zur Verfügung. Die Arbeitsaufträge sind dabei unterhalb der Grafik zu finden, im Unterrichtseinsatz empfiehlt es sich, die Grafik und die Arbeitsaufträge in unterschiedlichen Fernstern zur Verfügung zu haben.

die Verlängerung der Schlüssel nicht helfen. [6]

Für das Verständnis des später behandelten RSA-Verfahrens ist es zunächst notwendig, dass sich die Schülerinnen und Schüler über Eigenschaften der Prim- und Semiprimzahlen informieren. Dafür werden die Definitionen der (Semi)Primzahlen erläutert und ein Verfahren eingeführt, das das Auffinden von Primzahlen ermöglicht (Sieb des Eratosthenes)[7]. Anschließend sollen die Lernenden Semiprimzahlen in ihre Faktoren zerlegen, wobei sie erkennen, dass mit steigender Größe der Zahl der Aufwand der Faktorisierung immer höher wird – und irgendwann so groß ist, dass die Faktorisierung auch mit Hilfe eines Rechners nicht mehr durchzuführen ist.[8]

2.3 Asymmetrische Kryptologie mit RSA

Das 1978 entwickelte RSA-Verfahren ist ein asymmetrisches Verschlüsselungsverfahren. Die Größe der benutzten Semiprimzahlen ist variabel, so dass damit die nötige Sicherheit des Verfahrens gewährleistet werden kann (z. Zt. mind. 1024 Bit).

Da das RSA-Verfahren für die Lernenden meist nicht auf Anhieb zu verstehen ist, wurde dieser Unterrichtsabschnitt so gestaltet, dass zunächst händisch mit kleinen Zahlen operiert wird. Dabei berechnen die Schülerinnen und Schüler zunächst einen eigenen geheimen und öffentlichen Schlüssel und üben das Ver- und Entschlüsseln von Zahlen. Ein Arbeitsbogen zum modularen Rechnen führt die Schülerinnen und Schüler in diese für sie ungewohnte Rechenart ein.

Anschließend soll das Verfahren angewendet werden – auch hierbei wird mit kleinen Zahlen operiert, die noch per Hand zu berechnen sind: Die Schülerinnen und Schüler erhalten die Aufgabe, ihren Geburtstag (Monat und Tag einzeln) zu verschlüsseln. Sie tauschen zunächst ihren öffentlichen Schlüssel mit dem Nachbarn aus und nutzen den öffentlichen Schlüssel des Nachbarn, um den eigenen Geburtstag zu chiffrieren. Sie übermitteln das Chiffrat an ihren Nachbarn, der es mit seinem privaten Schlüssel

---

[6] Dieses Szenario bildet die Grundlage für den Film „Sneakers“ (http://de.wikipedia.org/wiki/Sneakers_%E2%80%93_Die_Lautlosen), bei dem der RSA-Miterfinder Len Adleman (das „A“ von RSA) als mathematischer Berater mitgewirkt hat.

[7] Für die bei realer RSA-Verschlüsselung benötigten sehr großen Primzahlen reicht dieses Verfahren nicht aus, hier kommt in der Regel der Miller-Rabin-Primzahltest zum Einsatz. Auf eine Implementierung dieses Tests können wir auf dem angestrebten Niveau nicht eingehen, allerdings steht in CrypTool eine fertige Implementierung als „Black Box“ zur Verfügung

[8] Für den Arbeitsbogen zum Sieb des Eratosthenes s. http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.3_asymmetrisch_verschluesseln/03%20Primzahlen%20finden%20mit%20dem%20Sieb%20des%20Eratosthenes.pdf

entschlüsselt[9].

Die RSA-Verschlüsselung ist nicht fixpunktfrei, d. h. es kann besonders bei kleinen Schlüsseln relativ häufig vorkommen, dass die Originalzahl und die verschlüsselte Zahl identisch sind. Das ist kein Argument gegen die Verwendung von RSA, weil es bei den tatsächlich eingesetzten Schlüssellängen nur selten auftritt und auch kein Sicherheitsrisiko darstellt – im Gegenteil: Die Fixpunktfreiheit der Enigma hat Alan Turing einen enscheidenden Ansatz zum Brechen des Enigma-Codes geliefert. Allerdings kann diese Tatsache in dieser Phase zu Fragen bei den Lernenden führen, die dann geklärt werden müssen.

Um die Einsicht zu motivieren, dass bei der Verschlüsselung mit RSA große Primzahlen gewählt werden sollten, wird nun im Plenum versucht, ein Chiffrat zu knacken. Zu diesem Zweck können einige Schülerinnen und Schüler (oder alle – je nach Größe des Kurses) ein Chiffrat zur Verfügung stellen. Gemeinsam versucht die Lerngruppe, den Modul n zu faktorisieren. Sind die beiden Faktoren gefunden, so kann das Produkt phi = (p-1) · (q-1) berechnet werden. Jetzt muss eine Zahl d (der geheime Schlüssel) gefunden werden, für die gilt: (d · e) mod phi = 1 [(e,n) ist der öffentliche Schlüssel.]. Mit dem gefundenen Schlüssel d kann nun das Chiffrat geknackt werden!

2.4 Sicherheit von RSA

Nachdem die Lernenden erfahren haben, dass die händische Anwendung des RSA-Verfahrens wegen der notwendigerweise sehr kleinen Schlüsselgrößen sehr unsicher ist, ist es nahe liegend, nunmehr Computer einzusetzen.

Deshalb führen die Schülerinnen und Schüler das RSA-Verfahren erneut durch, diesmal jedoch mit Zahlen, deren Größe so zu wählen ist, dass eine Entschlüsselung ohne Hilfe des Computers nicht durchzuführen ist. Die Rechnungen werden nun von den Lernenden mit Hilfe von CrypTool v1.4.30 (Menüpunkt Einzelverfahren => RSA-Kryptosystem => RSA-Demo) durchgeführt.

Hat man sein eigenes Schlüsselsystem mit der RSA-Demo erstellt, soll der öffentliche Schlüssel an den Kommunikationspartner geschickt werden, der damit sein Geburtsdatum – wie oben beschrieben – verschlüsseln soll. Die RSA-Demo bietet auch die Möglichkeit, nur mit dem öffentlichen Schlüssel eines Partners Nachrichten zu verschlüsseln. Nach einigen Übungen sind die Lernenden in der Lage, Nachrichten mit der RSA-Demo zu verschlüsseln und auch wieder zu entschlüsseln.[10]

---

[9] Arbeitsbogen zum RSA-Verfahren mit kleinen Zahlen (händische Lösung möglich): http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.3_asymmetrisch_verschluesseln/04%20RSA-Verschluesselung%20-%20Loesung.pdf

[10] Arbeitsbogen Anleitung zum Ver- und Entschlüsseln mit der RSA-Demo von CrypTool (mit Screenshots): http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.3_asymmetrisch_verschluesseln/06%20Anleitung%20Ver-%20und%20Entschluesseln%20mit%20der%20CrypTool-RSA-Demo.pdf

Mit der RSA-Demo kann aber auch aus einem bekannten öffentlichen Schlüssel der geheime Schlüssel bestimmt werden, wenn die Semiprimzahl zu klein gewählt wurde. Dieser Arbeitsschritt motiviert die nächste Aufgabe: „Wie groß muss der RSA-Schlüssel sein, damit er mit CrypTool nicht so schnell geknackt werden kann?“ Hier muss zunächst über die Bitlänge von Primzahlen und RSA-Schlüsseln gesprochen werden. Wenn man z. B. einen 128-Bit-RSA-Schlüssel erzeugen will, benötigt man zwei Primzahlen mit 64 Bit Länge. Wenn man mit diesen Werten experimentiert, zeigt sich, dass 128-Bit-Schlüssel noch sehr leicht mit CrypTool zerlegt werden können. Bei 256-Bit-Schlüsseln wird es schon schwieriger, 512-Bit-Schlüssel, die in der Praxis seit nunmehr 10 Jahren als unsicher gelten, können mit CrypTool v1 nicht mehr in vernünftiger Zeit geknackt werden.[11]

Nachdem die Frage beantwortet wurde, wie mittels Verschlüsselung Vertraulichkeit bei der E-Mail-Kommunikation hergestellt werden kann, steht nun die Frage nach der Integrität und Authentizität von Nachrichten im Mittelpunkt. Hierfür werden zum einen die notwendigen theoretischen Hintergründe erarbeitet (Hashwert, digitale Signatur), zum anderen üben sich die Schülerinnen und Schüler im Umgang mit einem echten Verschlüsselungssystem.

Mit dem Ende dieses Lernabschnitts haben die Lernenden die Fähigkeit erworben, selbstständig mit Verschlüsselungssystemen umzugehen, ihr eigenes Schlüsselpaar zu erzeugen und mit Programmen wie Thunderbird oder Outlook verschlüsselte und signierte E-Mails zu senden und zu empfangen.[12]

Die Verschlüsselung von E-Mails reicht nicht aus, um diesen Kommunikationsweg vollständig sicher zu gestalten. Trotz der Verschlüsselung einer E-Mail kann sich der Empfänger nicht sicher sein, ob eine Nachricht auch wirklich von dem Absender stammt, der im „Header“ der E-Mail genannt ist. Auch besteht noch die Gefahr, dass die Integrität einer E-Mail beschädigt wurde – d.h. dass Teile einer E-Mail entfernt, verändert oder hinzugefügt werden können. So besteht etwa die Gefahr, dass eine Nachricht, die – anscheinend oder tatsächlich – von einem bekannten Absender stammt, Schadcode, wie etwa ein infiziertes Dokument oder Programm enthält.

Um diese Gefahr zu beseitigen, wurde die digitale Signatur erfunden, die wie folgt funktioniert: Aus dem Text der E-Mail wird ein Hashwert (auch Streuwert bzw.

---

[11] Arbeitsbogen RSA knacken mit CrypTool (mit Screenshots): http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/3_verschluesseln/3.3_asymmetrisch_verschluesseln/07%20RSA%20knacken%20mit%20CrypTool.pdf
Bernhard Esslinger hat die mit CrypTool v1 möglichen Zerlegungen noch genauer eingegrenzt: Eine Semiprimzahl mit 315 Bit kann nicht zerlegt werden, ein RSA-Schüssel mit 235 Bit wird auf einem handelsüblichen Laptop mit dem quadratischen Sieb in knapp 41 Minuten zerlegt, die anderen implementierten Methoden haben bei dieser Länge keine Chance. Vgl. hierzu auch R.-H. Schulz, H. Witten: Zeit-Experimente zur Faktorisierung. In LOG IN Nr. 166/167 (2010), S. 113-120. http://page.mi.fu-berlin.de/rhschulz/Artikel_LogIn/Zeitexperimente.pdf

[12] Arbeitsbogen E-Mails verschlüsseln und digital unterschreiben http://medienwissenschaft.uni-bayreuth.de/inik/email_nur_fuer_dich/4_digital_unterschreiben/02%20AB%20E-Mails%20verschluesseln%20und%20digital%20unterschreiben.pdf

anschaulicher Fingerabdruck genannt) berechnet, den der Absender mit seinem privaten Schlüssel chiffriert. Jeder kann zwar mittels des öffentlichen Schlüssels des Senders diesen Hashwert entschlüsseln – es ist aber für jeden ersichtlich, dass die Verschlüsselung nur mit dem privaten Schlüssel des Senders erstellt worden sein konnte! Auf Empfängerseite wird der Hashwert der Nachricht erneut berechnet und mit dem empfangenen Hashwert verglichen. Sind diese beiden Werte unterschiedlich, so kann man davon ausgehen, dass die Integrität der Nachricht verletzt wurde.

Zuletzt bleibt nur noch folgendes Problem bestehen: Wie kann ich mir sicher sein, dass sich hinter dem öffentlichen Schlüssel eines Nutzers auch wirklich die Person verbirgt, mit der ich E-Mail-Kontakt habe? Schließlich kann sich jeder ein Schlüsselpaar erzeugen und eine fremde E-Mail-Adresse als die eigene bezeichnen.

Dieses Problem wird auf zwei unterschiedlichen Wegen gelöst: Zum einen gibt es so genannte Trust-Center, die Zertifikate ausstellen, in denen sie die Identität des Kommunikationsteilnehmers bestätigen. Ein solches Zertifikat ist kostenfrei für ein Jahr zu erhalten – wer es für einen längeren Zeitraum nutzen möchte, der muss zahlen. Zertifikate braucht man, wenn im Zuge von sicherer Email das Protokoll S/MIME (das z.B. in Thunderbird oder Outlook schon eingebaut ist) benutzt wird. Die andere Methode ist die Einbindung in ein „Web-of-Trust“. Hier bürgen jeweils Dritte für die Identität eines weiteren Teilnehmers im Web-of-Trust. Dadurch entsteht eine netzartige Struktur, in der jeder Teilnehmer für die Korrektheit einer bestimmten Anzahl von öffentlichen Signaturen bürgen kann. Die im Web-of-Trust signierten Schlüssel braucht man, wenn im Zuge von sicherer Email das Protokoll OpenPGP benutzt wird (z.B. mit Thunderbird/Enigmail).

3 Ausblick: RSA (fast) ohne Mathematik?

Die Beschäftigung mit RSA im Informatikunterricht stellt Schülerinnen und Schüler vor die schwierige Aufgabe, ein komplexes Verschlüsselungssystem nachvollziehen und anwenden zu können. Die Aufgabe der Lehrkraft ist dabei nicht minder schwer. Sie steht vor der Fragen: *Wie kann ich das Verfahren so aufbereiten, dass auch die Schülerinnen und Schüler es verstehen, die die mathematischen Hintergründe nicht vollständig durchdringen? Ab wann gilt das Verfahren als „verstanden“?*

Eine Möglichkeit, diese Fragen anzugehen, besteht in der Entwicklung eines pragmatischen Kompetenzstufen-Modells.[13] Auf der untersten Kompetenzstufe steht im vorliegenden Themenbereich RSA die Fähigkeit zur pragmatischen Nutzung von Verschlüsselungssystemen. Die vorliegende Unterrichtseinheit ist so konzipiert, dass auch ohne das Durchdringen der mathematischen Grundlagen ein Einblick in die Funktion des Verschlüsselungssystems gegeben wird. Am Anfang stehen die Entdeckung des Systems durch einfache händische Rechnungen und das Üben des Verschlüsselns anhand konkreter E-Mails. Im letzten Schritt der Einheit – dem

[13] Meyer, Hilbert: Leitfaden Unterrichtsvorbereitung, Berlin 2007. Vollständig überarbeitete Neuauflage.

computergestützten Umgang mit großen Primzahlen – werden die Grenzen der Sicherheit des Systems durch die Schülerinnen und Schüler entdeckt.

Ein pragmatisches Kompetenzstufenmodell zum Thema RSA schlagen wir wie folgt vor:

Stufe 0	Anwenden des Verschlüsselungssystems anhand der Verschlüsselung von E-Mails. Verstehen der Forderung nach Authentizität, Vertraulichkeit und Integrität beim Versenden von E-Mails.
Stufe 1	Verschlüsselung eines einfachen Datums durch die Anwendung kleiner Primzahlen für den Modul.
Stufe 2	Erkennen, dass bei der Nutzung kleiner Primzahlen keine ausreichende Sicherheit gewährleistet ist.
Stufe 3	Computergestütztes Suchen nach ausreichend großen Primzahlen, damit die Entschlüsselung eines Texts praktisch unmöglich wird.

Tab. 1 Pragmatisches Kompetenzstufenmodell zum Themenbereich „RSA“

Anhand der Tabelle lässt sich erkennen, dass wir ein erstes „Verstehen“ des RSA-Systems auf die Handhabung des Verschlüsselungsalgorithmus und das Verständnis der Anforderungen Authentizität, Vertraulichkeit und Integrität reduzieren. Die Benutzung von RSA ohne Mathematik setzt voraus, dass die benötigte Mathematik in einer „Blackbox“ versteckt wird. Dies passiert, wenn man z. B. Thunderbird mit den entsprechenden Kryptologie-Moduln für S/MIME bzw. OpenPGP/Enigmail verwendet (Stufe 0). Mit den in dieser Unterrichtsreihe vorgestellten Lernschritten und der Lernsoftware CrypTool wird das RSA-Verfahren zur „Greybox“. Als wichtigste mathematische Grundlage der Sicherheit der verwendeten asymmetrischen Verschlüsselung wird die Länge der im Schlüssel enthaltenen Semiprimzahl bzw. deren mögliche oder eben unmögliche Primfaktorzerlegung erkannt. Die eigentliche Ver- und Entschlüsselung erfolgt durch modulares Potenzieren, der verwendete Modul ist die erwähnte Semiprimzahl (Stufen 1-3). Die Aufgaben und Forschungsfragen, vor die die Schülerinnen und Schüler im Verlauf der Unterrichtseinheit gestellt werden, entsprechen den Stufen des Modells. Die Leistungsmessung der Schülerinnen und Schüler kann anhand der Einordnung in das Modell durchgeführt werden.

Mehr Mathematik als Primzahlen, Sieb des Eratosthenes sowie einfaches modulares Rechnen einschließlich Potenzieren kommt in dieser Unterrichtsreihe nicht zum Einsatz. Für ein vollständiges mathematisches Durchdringen fehlen noch die folgenden Schritte, wenn das RSA-Verfahren zur „Whitebox“ werden soll[14]:

- Für das modulare Potenzieren werden einfache Regeln des modularen Rechnens sowie der „Square-and-Multiply“-Algorithmus zum schnellen Potenzieren

[14] Einen Überblick über die zum vollständigen Verständnis benötigten mathematischen Grundlagen erhält man in der Artikelserie „RSA&Co. in der Schule – Neue Folge“ von H. Witten und R.-H. Schulz aus der Zeitschrift LOG IN. Links zu den einzelnen Artikeln dieser Folge findet man unter https://www.cryptoportal.org/ => Linksammlung => RSA&Co.

verwendet (s. RSA&Co., Neue Folge Teil 1: „RSA für Einsteiger“).

- Zur Berechnung der Schlüssel benötigt man bei großen Zahlen den erweiterten Euklidischen Algorithmus. Außerdem kann man sich fragen, warum modulare Addition oder Multiplikation kein sicheres Verschlüsselungssystem liefert, warum man also Potenzieren muss (s. RSA&Co., Neue Folge Teil 2: „RSA für große Zahlen“).

- Für den Beweis der Korrektheit des RSA-Verfahrens verwendet man den kleinen Satz von Fermat bzw. den Satz von Euler-Fermat oder auch den Satz von Carmichael (s. RSA&Co., Neue Folge Teil 3: „RSA und die elementare Zahlentheorie“).

- Wie man seit dem Altertum weiß, gibt es zwar unendlich viele Primzahlen, die sind aber mit zunehmender Größe immer dünner gesät. Gibt es bei der milliardenfachen Kommunikation überhaupt genügend Primzahlen für RSA? (s. RSA&Co., Neue Folge Teil 4: „Gibt es genügend Primzahlen für RSA?“). Die Antwort auf diese Frage liefert der Gaußsche Primzahlsatz[15], der eng mit der berühmten Riemannschen Vermutung[16] verknüpft ist, vielleicht das aktuell wichtigste ungelöste mathematische Problem.

- Bei der Größe der heute benötigten Schlüssel reichen klassische Methoden zum Auffinden von Primzahlen nicht mehr aus. Man verwendet hierfür den Miller-Rabin-Primzahltest. Doch wie funktioniert der? (s. RSA&Co., Neue Folge Teil 5: „Der Miller-Rabin-Primzahltest oder Falltüren für RSA mit Primzahlen aus Monte Carlo“)

- Wie ist es um die Sicherheit von RSA bestellt? Erste Antworten dazu erhält man im o. e. Artikel von Schulz/Witten „Zeitexperimente zur Faktorisierung“, weitere mögliche Angriffe gegen RSA und die entsprechenden Vorkehrungen dagegen findet man in jedem Standardwerk zur Kryptologie (z. B. Klaus Schmeh: Kryptografie – Verfahren, Protokolle, Infrastrukturen).

Wie wir eingangs erwähnt haben, können die Jugendlichen zwar mit E-Mail-Programmen umgehen und tun dies auch häufig, ein Problembewusstsein über die damit verbundenen Fragen der Computersicherheit fehlt allerdings fast immer. Aber auch die Erwachsenen tun sich mit der sicheren Kommunikation per E-Mail schwer. Aus diesem Grund haben die Post mit dem E-Postbrief[17] und die Bundesregierung mit DE-Mail[18] kostenpflichtige Dienste ins Leben gerufen, die ein hohes Maß an Sicherheit versprechen.

[15] http://de.wikipedia.org/wiki/Primzahlsatz
[16] http://de.wikipedia.org/wiki/Riemannsche_Vermutung
[17] http://de.wikipedia.org/wiki/E-Postbrief
[18] http://de.wikipedia.org/wiki/De-Mail

Um solche Angebote kritisch bewerten zu können, bedarf es einer Grundbildung in Fragen der Computersicherheit, die über das Verständnis und ggf. die Programmierung des Caesar-Verfahrens hinausgeht. Mit unserer Unterrichtsreihe wollen wir einen u. E. wichtigen Baustein zum Verständnis der asymmetrischen Kryptographie liefern, der schon in der Sekundarstufe I erarbeitet werden kann und somit potenziell allen Schülerinnen und Schülern zur Verfügung steht. Eine ausführlichere und mathematisch-informatisch fundiertere Behandlung des RSA-Verfahrens wird in der Regel erst in der Oberstufe möglich sein.