Informatik im Kontext

E-Mail (nur?) für Dich

Eine Unterrichtsreihe des Projekts

Informatik im Kontext

Autoren:

Andreas Gramm, Malte Hornung und Helmut Witten

Beilage zu LOG IN, 31. Jg. (2011), Heft Nr. 169/170

0

Inhalt

E-Mail (nur?) für Dich 3

1 Wie kommt eine E-Mail von meinem Computer auf den Computer des Empfängers? 6

1.1 Bezug zu den Bildungsstandards 6
1.2 Ein eigenes Protokoll entwerfen 6
1.3 E-Mail-Protokolle mit einem Netzwerkanalyse-Werkzeug erfassen und rekonstruieren 6

2 Gefahren bei der Kommunikation über öffentliche Medien erkennen . . 8

2.1 Bezug zu den Bildungsstandards 8
2.2 Entdecken der Gefahren und Formulieren von Sicherheitsanforderungen 8

3 Verschlüsselung erreicht Vertraulichkeit 9

3.1 Bezug zu den Bildungsstandards 10
3.2 Monoalphabetische Kryptographie – Caesars Geheimcode 10
3.3 Polyalphabetische Kryptographie – Vigenère 10
3.4 Trennung von Ver- und Entschlüsseln mittels Falltürfunktion 11
3.5 Das Prinzip der asymmetrischen Kryptologie 11
3.6 Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und Zerlegen in Primfaktoren 12
3.7 Implementierung asymmetrischer Kryptologie in RSA 12
3.8 Sicherheit von RSA 13

4 Integrität der Nachricht und Authentizität des Absenders mit digitaler Unterschrift prüfen 14

4.1 Bezug zu den Bildungsstandards 15
4.2 Das Prinzip der digitalen Unterschrift entdecken 15
4.3 Digitale Unterschrift anwenden 15

5 Warum sollte ich sicher kommunizieren? 16

5.1 Bezug zu den Bildungsstandards 16
5.2 Gruppenpuzzle zur Kommunikationsfreiheit 16

In dieser Unterrichtsreihe eingesetzte Software 18
Literatur und Internetquellen 18

E-Mail (nur?) für Dich

Eine Unterrichtsreihe des Projekts *Informatik im Kontext*

von Andreas Gramm, Malte Hornung und Helmut Witten

E-Mail (nur?) für Dich *ist der Titel einer Unterrichtsreihe, die – das deutet die zweideutige Formulierung bereits an – die Erarbeitung von Grundlagen der Kommunikation in Computernetzwerken mit der Frage nach der Vertraulichkeit solcher Kommunikation verbindet. Mit der Diskussion verschiedener Aspekte des vieldimensionalen Kontexts der sicheren Kommunikation über öffentliche Kanäle folgt die Reihe dem Prinzip der Kontextorientierung, für das zuletzt durch das Projekt Informatik im Kontext (IniK) geworben wird (Koubek u.v.a., 2011; siehe auch Abbildung 1). Nach einer kurzen Vorstellung der Kontextorientierung werden die einzelnen Lernabschnitte der Reihe und eingesetzte Materialien beschrieben. Damit wollen die Autoren dieser Broschüre vor allem eines erreichen: den Leserinnen und Lesern Lust machen, die Reihe »E-Mail (nur?) für Dich« im Informatikunterricht in Teilen oder ganz durchzuführen!*

Das fachdidaktische Prinzip der Kontextorientierung fordert die Orientierung von Informatikunterricht an sinnstiftenden Kontexten (vgl. Koubek u.a., 2009). Konzeptuell ist IniK an Kontext-Projekte in den Naturwissenschaften wie *Chemie im Kontext* (CHiK), *Biologie im Kontext* (bik) und *Physik im Kontext* (piko) angelegt. Neben der Orientierung an Kontexten werden die Orientierung an Bildungsstandards wie den Empfehlungen der *Gesellschaft für Informatik* (AKBSI, 2008) und eine Vielfalt schüleraktivierender Methoden als weitere Prinzipien eines erfolgreichen kontextorientierten Unterrichts beschrieben. Damit wird die Orientierung an sinnstiftenden Kontexten auch zum Anlass genommen, generell informatische Bildung weiterzuentwickeln.

Neben der konzeptuellen Präzision und Weiterentwicklung (vgl. Engbring/Pasternak, 2010) werden von der bundesweit aktiven, offenen Arbeitsgruppe seit einigen Jahren Unterrichtsreihen entwickelt und getestet, um so exemplarisch die Umsetzbarkeit des Konzepts zu demonstrieren. Für fünf der vorgeschlagenen Kontexte wurden inzwischen detailliert Unterrichtsreihen ausgearbeitet und von Koubek u.v.a. (2011) veröffentlicht: Die Reihe *Chatbots* widmet sich dem Thema der künstlichen Intelligenz (vgl. Witten/Hornung, 2008 u. 2009). Mit der an der Universität Hamburg entwickelten integrierten Entwicklungsumgebung für Sprachdialogsysteme *inES* lernen Schülerinnen und Schüler eine sprachgesteuerte Informatikanwendung zu entwickeln, wie sie uns heute mittlerweile in Mobiltelefonen, Navigationsgeräten oder natürlichsprachlichen Informations- und Auskunftssystemen im Alltag begegnen (vgl. Breier u.a., 2008). Ausgearbeitet wurde des Weiteren eine Reihe zum Thema *Datenschutz im Web 2.0,* in deren Zentrum ein Online-Planspiel zu sozialen Netzwerken steht. In einer Reihe zur *RFID-Technologie* werden neben der Erarbeitung der technischen Grundlagen auch gesellschaftliche Auswirkungen einer möglichen Überwachung durch RFID-Chips auf Chipkarten thematisiert. Derzeit in der Entwicklung befindet sich in Kooperation mit der Freien Universität Berlin eine Reihe zur *Kommunikation in Mobilfunknetzen*.

Ausgehend von der Frage, wie eigentlich eine E-Mail von einem Rechner zum ande-

Abbildung 1:
Die Webseite des Projekts »Informatik im Kontext« mit interessanten Unterrichtsreihen und Materialien:
http://www.informatik-im-kontext.de/

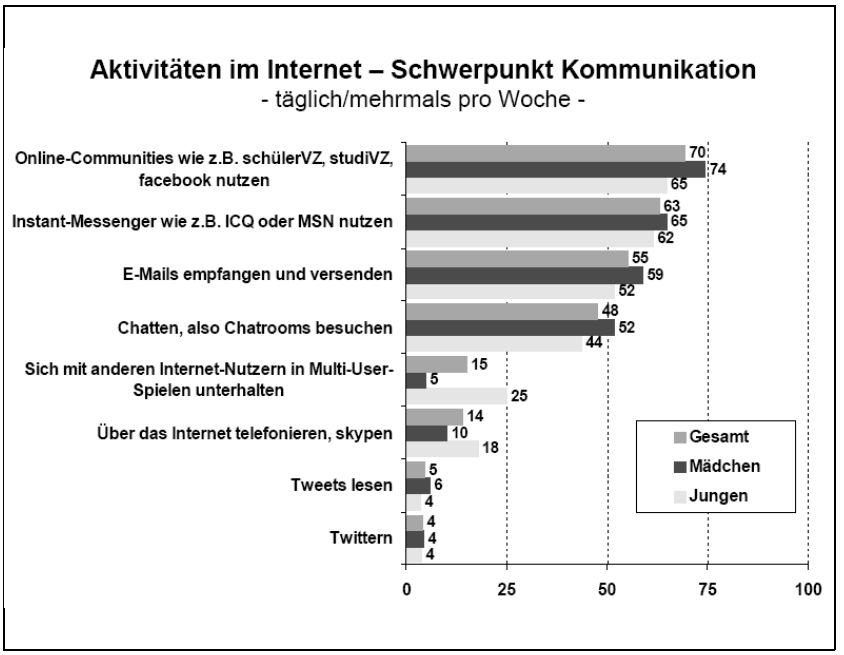


Abbildung 2:
Die JIM-Studie 2010 bestätigt: Jugendliche verbringen viel Zeit im Internet mit Kommunikation und nutzen dabei häufig E-Mail.

Quelle: mpfs, 2010, S. 30;
Angaben in Prozent (Basis: alle Befragten, n = 1.208)

ren gelangt, führt die Unterrichtseinheit »E-Mail (nur?) für Dich« die Schülerinnen und Schüler in den Kontext der privaten Kommunikation über öffentliche Computernetzwerke ein. Dabei identifizieren die Lernenden Gefahren und entdecken Sicherheitsmaßnahmen, um ihre eigene Kommunikation zu schützen.

Angriffe auf E-Mail-Konten und E-Mail-Verkehr stellen heutzutage eine ernstzunehmende Gefahr dar. Die Intentionen der Hacker können dabei durchaus differieren: Hauptgrund für einen Angriff ist meist die Hoffnung auf monetären Gewinn. Ist das E-Mail-Konto erst gehackt, so ist der Weg offen, weitere Systeme des Kontoinhabers, wie etwa Online-Banken (Neteller, Moneybookers, etc.) oder andere Systeme, die eine Umwandlung von virtueller in reale Währung ermöglichen (»MMORPGS«, Glücksspielseiten u. Ä.), anzugreifen. Ein weiterer Beweggrund kann politische oder Industrie-Spionage sein. Zuletzt können Hacks auch aus rein destruktiven Gründen durchgeführt werden.

Der Lerngegenstand ist den Schülerinnen und Schülern nicht fremd: Trotz des Vormarschs von sozialen Netzwerken und Chatprogrammen kommunizieren Jugendliche noch immer verstärkt via E-Mail, wie die jüngste JIM-Studie (mpfs, 2010) zeigt (siehe Abb. 2). Die Unterrichtsreihe knüpft an dieser Stelle an: Sie verbindet ein bereits bekanntes Informatiksystem mit neuen Fragestellungen und motivierenden Forschungsaufgaben, um den Schülerinnen und Schülern zu ermöglichen, bereits erworbenes Wissen konstruktiv in noch unbekannten Gebieten – wie etwa der Kryptologie – anzuwenden. Darüber hinaus erscheint das Thema in hohem Maße gendergerecht, da der E-Mail-Dienst des Internets von Mädchen noch etwas stärker zu Kommunikationszwecken genutzt wird als von ihren Mitschülern.

Die Reihe setzt das Konzept von *Informatik im Kontext* wie folgt um:

1. Mit dem Thema »Sichere Kommunikation über öffentliche Netzwerke« wurde ein vieldimensionaler Kontext gewählt. Dabei entstammt die E-Mail-Technologie aus dem unmittelbaren Lebensumfeld von Schülerinnen und Schülern.
2. Es werden gezielt Kompetenzen aus verschiedenen der in den Bildungsstandards der GI (AKBSI, 2008) beschriebenen Kompetenzbereichen gefördert. Schwerpunktmäßig konzentriert sich die Unterrichtseinheit jedoch auf die Bereiche:
   - Inhaltsbereich *Informatiksysteme*,
   - Inhaltsbereich *Informatik, Mensch und Gesellschaft*,
   - Prozessbereich *Begründen und Bewerten*.
3. Die Reihe zeichnet sich durch eine Vielfalt an schüler- und handlungsorientierten Methoden wie z. B. entdeckendem Lernen und Gruppenpuzzle aus.

Die Unterrichtsreihe »E-Mail (nur?) für Dich« führt zunächst in Grundlagen der technischen Realisierung von Kommunikation über öffentliche Netzwerke ein. Bei der Analyse von Netzwerkverkehr zur Rekonstruktion der E-Mail-Protokolle SMTP und POP3 wird deutlich, dass beim Beibehalten aller Standardeinstellung basale Sicherheitsanforderungen wie Vertraulichkeit oder Integrität und Authentizität einer Nachricht nicht gegeben sind. Mögliche Gefahrensituationen werden im Computerraum der Schule simuliert, um so die Erarbeitung verschiedener Verfahren der Kryptologie zu motivieren. Neben z. T. unzulänglichen klassischen Verfahren wird gezeigt, wie mit dem asymmetrischen Verfahren RSA neben der Vertraulichkeit auch die Forderung nach Integrität und Authentizität mittels digitaler Unterschriften erfüllt werden kann. Während in den regulären Stunden gewonnene Erkenntnisse aufeinander aufbauen, werden an einigen Stellen Anregungen für optionale, vertiefende Exkurse angeboten.

Dabei stehen folgende Fragestellungen im Fokus, die jeweils Ausgangspunkt für das Erarbeiten eines Lernabschnitts darstellen (siehe Abb. 3):

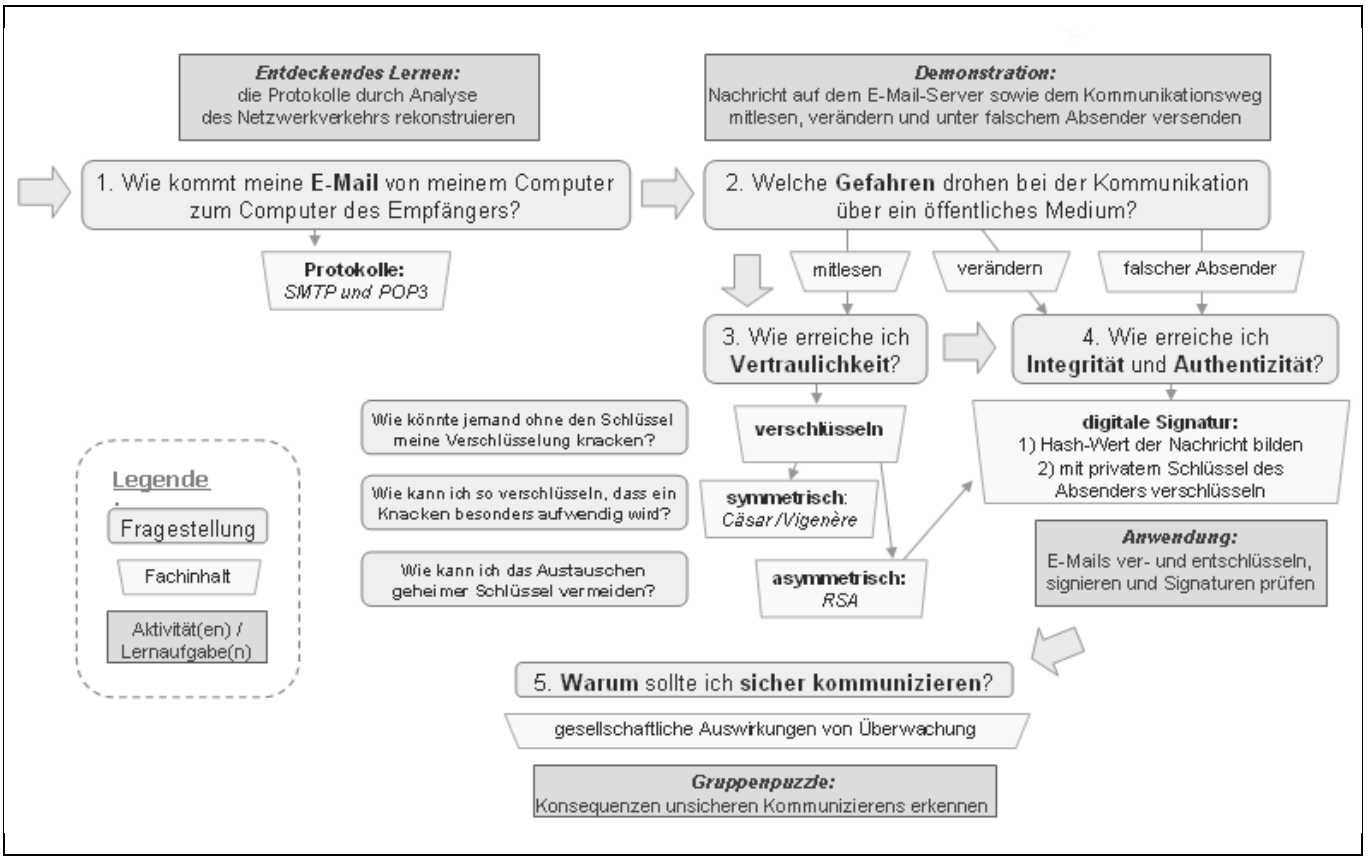


Abbildung 3 (oben):
Zentrale Lernabschnitte, Fachinhalte und Lernhandlungen im Überblick.

1. Wie kommt eine E-Mail von meinem Computer zum Computer des Empfängers?
2. Welche Gefahren bestehen bei der Kommunikation über öffentliche Medien?
3. Wie kann ich mit Verschlüsselung Vertraulichkeit herstellen?
4. Wie kann ich mit einer digitalen Unterschrift die Integrität der Nachricht und die Authentizität des Absenders überprüfen?
5. Warum sollte ich sicher kommunizieren?

Diese Lernabschnitte können unterschiedlich intensiv bearbeitet werden. Über die Auswahl einzelner *Module* kann der zeitliche Aufwand für die Erarbeitung im Unterricht so flexibel angepasst werden, es muss also nicht immer gleich der gesamte Umfang an vorgeschlagenem Material erarbeitet werden.

Die Abbildung 4 bietet einen Überblick über mögliche Lernpfade.

Als *Vorkenntnis* sollten die Schülerinnen und Schüler bereits wissen, dass jeder an das Internet angeschlossene Computer sich über eine eindeutige IP-Adresse identifizieren lässt und Nachrichten solange von einem Compu-

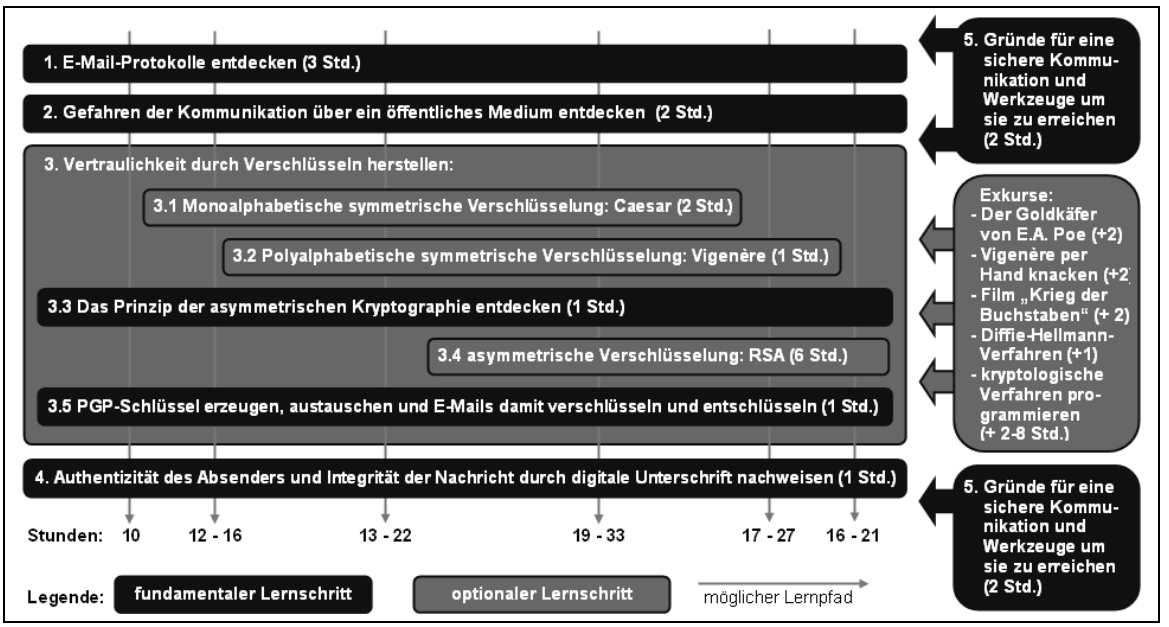


Abbildung 4 (unten):
Mögliche Lernpfade – Modul-Auswahl für die kontextorientierte Unterrichtsreihe »E-Mail (nur?) für Dich«.

ter an Nachbarcomputer weitergeleitet werden, bis sie beim Computer des Empfängers eingetroffen sind. Sollten die Schülerinnen und Schüler nicht über diese Vorkenntnisse verfügen, lassen sich diese z. B. mit der Sachgeschichte der »Sendung mit der Maus« zum Thema *Internet* (wdr, o.J.), dem Rollenspiel »Wie funktioniert das Internet?« von Andreas Gramm (2009) bzw. der interaktiven Lernumgebung FILIUS (Freischlad/Stechert, 2011) mit passenden Szenarien zur Simulation von E-Mail-Verkehr erarbeiten.

1

Wie kommt eine E-Mail von meinem Computer auf den Computer des Empfängers?

Wer Gefahren und Risiken der E-Mail-Kommunikation identifizieren will, muss zunächst die technischen Abläufe verstehen, um mögliche Angriffspunkte erkennen zu können. In entdeckendem Lernen erarbeiten die Schülerinnen und Schüler in diesem Schritt zunächst das Konzept eines Kommunikationsprotokolls und lernen exemplarisch zwei typische E-Mail-Protokolle kennen.

Bezug zu den Bildungsstandards

Die Schülerinnen und Schüler …
- ▷ verstehen die Grundlagen des Aufbaus von Informatiksystemen und deren Funktionsweise.
- ▷ nutzen Diagramme, Grafiken und Modelle, um sich informatische Sachverhalte selbstständig zu erarbeiten.
- ▷ verknüpfen informatische Inhalte und Vorgehensweisen mit solchen außerhalb der Informatik.

Ein eigenes Protokoll entwerfen

Am Anfang wird auf einen Einstieg über die technische Ebene verzichtet. In Anlehnung an eine Unterrichtsidee von Werner Arnhold (Fritz-Karsen-Schule, Berlin) werden die Lernenden aufgefordert, in Gruppen jeweils ein Verfahren zu entwickeln, um mit einer unter einer Tür verlaufenden Schnur (ohne zu sprechen und ohne weitere Gegenstände) ein Wort zu kommunizieren! Als Hilfsmittel für schwächere Gruppen können dazu z. B. der Morsecode oder eine durchnummerierte Aufstellung der Buchstaben des Alphabets bereitgehalten werden. Im Plenum werden dann einige der Verfahren vorgeführt. In der Diskussion von Gemeinsamkeiten und Unterschieden sowie Vor- und Nachteilen der verschiedenen Verfahren werden zentrale Aspekte von Protokollen wie z. B. die Übertragungsgeschwindigkeit, Fehleranfälligkeit oder Steuerungssignale wie »habe den letzten Buchstaben nicht erkannt« genannt. So erkennen die Schülerinnen und Schüler, warum ein Protokoll für den Erfolg einer Kommunikation mittels Austausch von Information über Entfernungen hinweg nötig ist und was ein gutes Protokoll ausmacht. Abschließend sollte der Begriff »Protokoll« (in Abgrenzung zu der weitläufig verbreiteten Bedeutung eines Berichts) als Fachbegriff eingeführt werden, der für die »Regeln für eine Kommunikation« steht.

E-Mail-Protokolle mit einem Netzwerkanalyse-Werkzeug erfassen und rekonstruieren

Durch die Analyse von authentischem Netzwerkverkehr entdecken die Schülerinnen und Schüler die E-Mail-Protokolle SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*) zum Versenden und POP3 (***P**ost **O**ffice **P**rotocol Version 3*) zum Empfangen von E-Mails.

Die Schülerinnen und Schüler erhalten für eines der beiden Protokolle eine ungeordnete Liste von Nachrichten (siehe Abb. 6) und den Auftrag, anhand des beobachteten Netzwerkverkehrs die Nachrichten dem E-Mail-Client und dem

E-Mail-Server zuzuordnen und in die korrekte Reihenfolge zu bringen sowie einzelnen Abschnitten der Kommunikation übergeordnete Begriffe wie »Benutzer anmelden« oder »Verbindung beenden« zuzuordnen. Nun kann der E-Mail-Server auch direkt über Telnet angesprochen werden und versucht werden, gemäß dem rekonstruierten Protokoll eine E-Mail zu versenden oder E-Mails anzeigen zu lassen. Im Austausch mit einem Partner werden Gemeinsamkeiten und Unterschiede der beiden Protokolle erörtert.

Da in diesem Zusammenhang E-Mails und Passwörter sichtbar werden, ist es unbedingt notwendig in einer didaktischen Umgebung einen fiktiven und somit geschützten Raum zu verwenden, der nicht die reale Privatsphäre der Schülerinnen und Schüler betrifft. Dazu bietet es sich an, für die Doppelstunde einen eigenen E-Mail-Server auf einem Rechner des Computerraums zu starten und dort Benutzerkonten für die Schülerinnen und Schüler anzulegen, für die sie dann ihren E-Mail-Client einrichten. Hier bietet sich (leider nur für Windows-Systeme) der E-Mail-Server *Hamster* von Volker Gringmuth an, der sich z.B. auf einem USB-Stick installieren lässt, sodass der Server nur jeweils in den Unterrichtsstunden zu dieser Reihe verfügbar ist.

Der Einsatz eines Netzwerkanalysewerkzeugs könnte theoretisch unter den Geltungsbereich des sogenannten »Hacker-Paragraphen« (§ 202c StGB) fallen. Das Bundesverfassungsgericht hat jedoch festgestellt, dass das Gesetz nicht anzuwenden ist, wenn kein Vorsatz einer schadhaften Handlung vorlegt. Der Einsatz zu Zwecken der Lehre ist somit statthaft, solange Schülerinnen und Schüler darauf hingewiesen werden, dass die Anwendung außerhalb eines eigenen Netzwerks (z.B. Port-Scannen auf Rechnern im Internet) eine strafbare Handlung darstellen kann (vgl. BVerfG, 2009). Darüber hinaus wird mit *SocketSniff* bewusst ein Werkzeug mit sehr begrenzten Möglichkeiten vorgeschlagen.

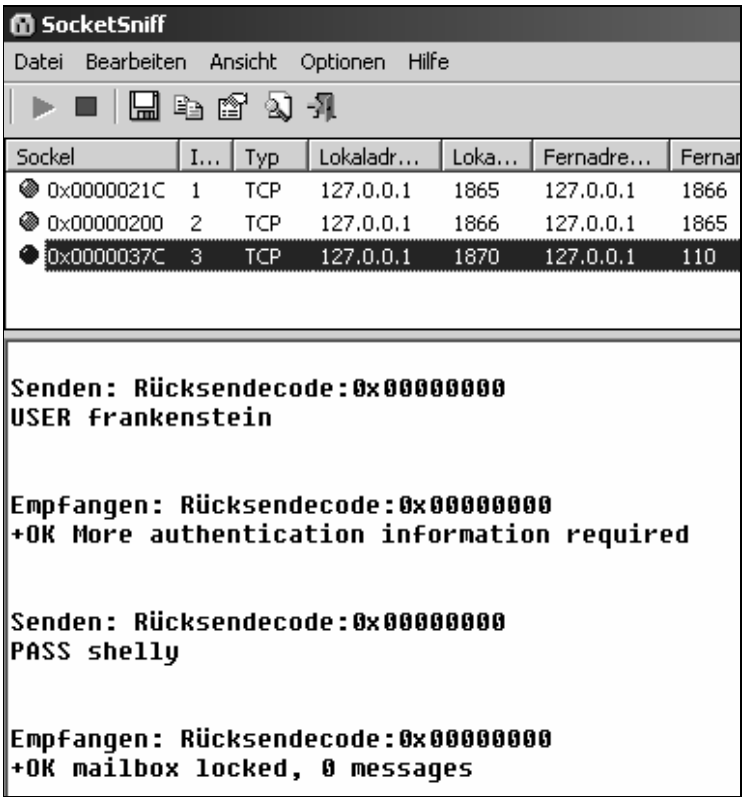


Abbildung 5: Protokoll des Authentifizierungsvorgangs.

Abbildung 6: Ungeordnete Nachrichten und Schritte der Kommunikation zum Abrufen neuer E-Mails.

2 Gefahren bei der Kommunikation über öffentliche Medien erkennen

In diesem Lernabschnitt werden die Schülerinnen und Schüler in einer fiktiven Situation verschiedene reale Gefahren der Kommunikation im Internet erleben. Dazu senden sie sich erneut Nachrichten über einen auf dem Lehrerrechner gestarteten E-Mail-Server. Zu Beginn des Unterrichtsblocks empfangen die Schülerinnen und Schüler eine E-Mail, deren Absender sich offensichtlich als jemand anderes ausgibt (z.B. die Bundeskanzlerin). Ausgehend von einer ersten Einordnung der E-Mail (»Hier geht etwas nicht mit rechten Dingen zu!«) bekommen die Schülerinnen und Schüler den Auftrag zu beobachten, wie die Lehrerin bzw. der Lehrer die Kommunikation stört.

So soll der Lernabschnitt die Schülerinnen und Schüler für die Gefahren bei der Nutzung von E-Mail-Systemen sensibilisieren. Ziel ist, dass die Schülerinnen und Schüler erkennen, dass elektronische Kommunikation die gleichen Anforderungen erfüllen sollte wie die Kommunikation per Post: Vertraulichkeit, Integrität und Authentizität.

Bezug zu den Bildungsstandards

Die Schülerinnen und Schüler …
- ▷ reagieren angemessen auf Risiken bei der Nutzung von Informatiksystemen.
- ▷ stellen Fragen und äußern Vermutungen über informatische Sachverhalte.
- ▷ gewichten verschiedene Kriterien und bewerten deren Brauchbarkeit für das eigene Handeln.

Entdecken der Gefahren und Formulieren von Sicherheitsanforderungen

Das *Vortäuschen einer falschen Identität* auf der Client-Seite geschieht über die Manipulation des E-Mail-Headers. Dieser enthält Informationen über den Absender, den Empfänger, das Datum und den Weg der E-Mail. E-Mail-Clientprogramme wie Outlook oder Thunderbird lassen hier frei editierbare Angaben zu, die vom versendenden E-Mail-Server oft nicht überprüft werden.

Um das *Mitlesen von E-Mails* (inklusive übermittelter Passwörter) in einem »man-in-the-middle«-Spionageangriff auf dem Kommunikationsweg realistisch demonstrieren zu können, wird empfohlen, einen Standardrechner mithilfe einer zusätzlichen Netzwerkkarte (und der detaillierten Anleitung in den Materialien zu dieser Reihe; siehe Anmerkung auf Seite 17) in wenigen Schritten in eine Netzwerkbrücke umzubauen. Der so manipulierte Rechner symbolisiert dann einen Vermittlungsrechner (Router). Ist ein Umbau zum »Router« nicht möglich, so kann alternativ ein ähnlicher Angriff auf dem Lehrerrechner simuliert werden – nur ist die Trennung zwischen den Rollen Kommunikationsinfrastruktur und Diensterbringer dann nicht mehr deutlich erkennbar. Das Mitlesen der Passwörter für die E-Mail-Konten ist mit *SocketSniff* nicht möglich. Hier bietet sich das wesentlich mächtigere Netzwerkanalysewerkzeug *Wireshark* an, dessen Nutzung aus naheliegenden Gründen (vgl. BVerfG, 2009) nur für Lehrende vorgesehen ist.

Das dritte Szenario simuliert, welche Auswirkungen es hat, wenn ein

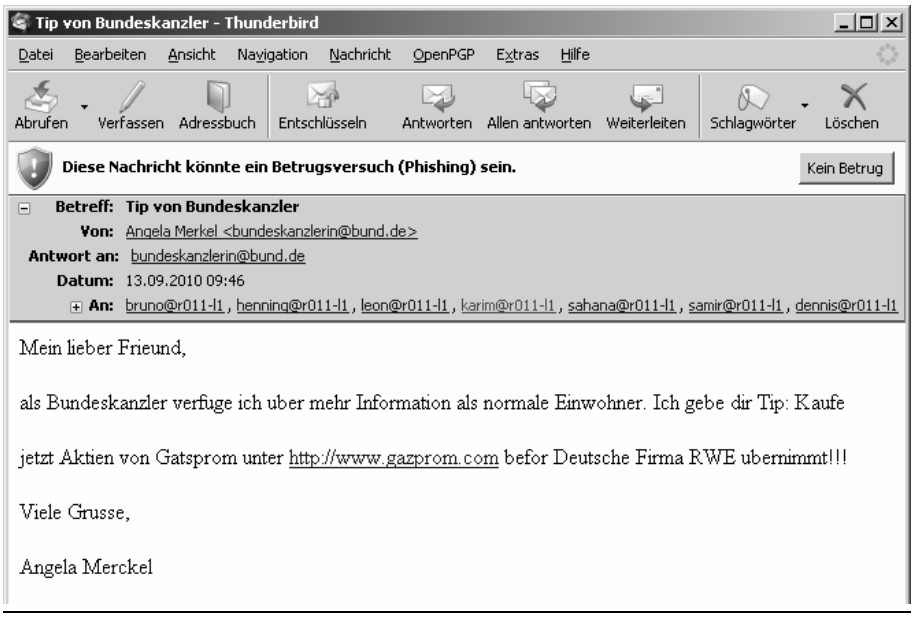


Abbildung 7:
Eine E-Mail mit zwielichtiger Intention und gefälschtem Absender – oder sind Sie mit der Bundeskanzlerin befreundet?

Angreifer direkten Zugriff auf einen E-Mail-Server besitzt. Auf dem Server befinden sich alle gesendeten und empfangenen Nachrichten des Clients (sofern dieser sie nicht gelöscht hat). Besitzt ein Angreifer Zugriff auf diese Daten, so kann er die *E-Mails* nicht nur mitlesen, sondern sie auch nach Belieben *manipulieren*.

Verschlüsselung erreicht Vertraulichkeit

3

Im vorangegangenen Lernabschnitt wurde versucht, die Lernenden für die Frage zu sensibilisieren, wie bei der E-Mail-Kommunikation Vertraulichkeit hergestellt werden kann. Die Antwort auf diese Frage liegt nahe: Verschlüsselung!

Anmerkung: Auf der Abbildung zur Modul-Auswahl für diese Unterrichtsreihe (Abb. 4, S. 5) wurden folgende Module als *optional* gekennzeichnet: 3.1 (Monoalphabetische Verschlüsselung am Beispiel Caesar), 3.2. (Polyalphabetische Verschlüsselung am Beispiel Vigenère) und 3.3 (Asymmetrische Verschlüsselung am Beispiel RSA). In der Tat können die Ergebnisse dieser Lernschritte z. B. in einem Lehrervortrag vermittelt werden, wenn nur wenig Zeit zur Verfügung steht. Eine weitere Möglichkeit ergibt sich, wenn die Kryptologie als selbstständige Unterrichtsreihe außerhalb dieser Einheit behandelt wird. Diese Möglichkeit wäre dann vorzuziehen, wenn die Kryptologie mit umfänglichen Programmierübungen verbunden werden soll. Allerdings geht dann der Kontext »E-Mail« verloren. Nach unseren Erfahrungen hat es sich für die Lernenden als sehr motivierend erwiesen, wenn die Übungen zum Ver- und Entschlüsseln und ggf. »Knacken« einer Chiffre in einem simulierten E-Mail-Kontext innerhalb des Klassenraums durchgeführt werden. Andererseits lässt sich das Thema »Kryptologie« in vielfacher Hinsicht durch Exkurse ausweiten und anreichern (siehe Kasten am Rand).

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 von 25 beim Caesar-Verfahren erheblich:

$$26! = 403.291.461.126.605.635.584.000.000.$$

Bei dieser astronomisch hohen Anzahl ist ein systematisches Ausprobieren aller Schlüssel 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 länger als 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 zur Entschlüsselung führen (vgl. z. B. das Projekt VENONA, das aufgrund fehlerhafter One-Time-Pad-Verschlüsselung zur Enttarnung mehrerer sowjetischer Atomspione in den USA führte; s. a. http://de.wikipedia.org/wiki/VENONA-Projekt).

Aufbewahrung und Transport der geheimen Schlüsselwörter stellte selbst für Geheimdienste im 20. Jahrhundert eine große Herausforderung dar. Mit der asymmetrischen Kryptographie wurden in der zweiten Hälfte des 20. Jahrhunderts Verfahren entwickelt, die ohne den vorherigen Austausch geheimer Schlüssel auskommt. Das bekannteste Verfahren RSA wird heute in vielen Web-Sicherheits-Technologien wie SSL/TSL benutzt, um Sitzungsschlüssel für eine symmetrische Verschlüsselung auf sicherem Wege auszutauschen.

Mögliche Exkurse zum Thema »Kryptologie«

Für den Fall, dass mehr Zeit für die Erarbeitung vertiefender Aspekte zur Kryptologie bereitsteht, wird Material zu verschiedenen optionalen Exkursen angeboten:

- ▷ Einstieg in die Kryptologie mit der Geschichte »Der Goldkäfer« von Edgar Allan Poe.
- ▷ Einen mit Vigenère verschlüsselten Text per Hand knacken.
- ▷ Auswerten des BBC-Dokumentarfilms »Krieg der Buchstaben«.
- ▷ Erarbeiten der mathematischen Umsetzung des Diffie-Hellman-Verfahrens.
- ▷ Programmieren einzelner kryptologischer Verfahren (eine grafische Benutzungsoberfläche und Informationstexte zur Bearbeitung von Zeichenketten werden zurzeit erarbeitet).

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

Abbildung 8:
Doppelalphabet-Streifen für das Ver- und Entschlüsseln nach dem Caesar-Verfahren.

Bezug zu den Bildungsstandards

Die Schülerinnen und Schüler …
- ▷ erkennen die Unsicherheit einfacher Verschlüsselungsverfahren.
- ▷ strukturieren Sachverhalte durch zweckdienliches Zerlegen und Anordnen.
- ▷ kennen Algorithmen zum Lösen von Aufgaben und Problemen aus verschiedenen Anwendungsgebieten und lesen und interpretieren gegebene Algorithmen.

Monoalphabetische Kryptographie – Caesars Geheimcode

Die Schülerinnen und Schüler werden aufgefordert, sich gegenseitig mithilfe von je zwei untereinander angeordneten und seitlich gegeneinander verschobenen Doppelalphabet-Streifen (siehe Abb. 8) verschlüsselte Nachrichten per E-Mail zuzusenden und erhaltene Nachrichten zu entschlüsseln. Dabei lernen die Schülerinnen und Schüler erste Fachbegriffe aus der Kryptologie kennen und wenden diese sachgerecht an.

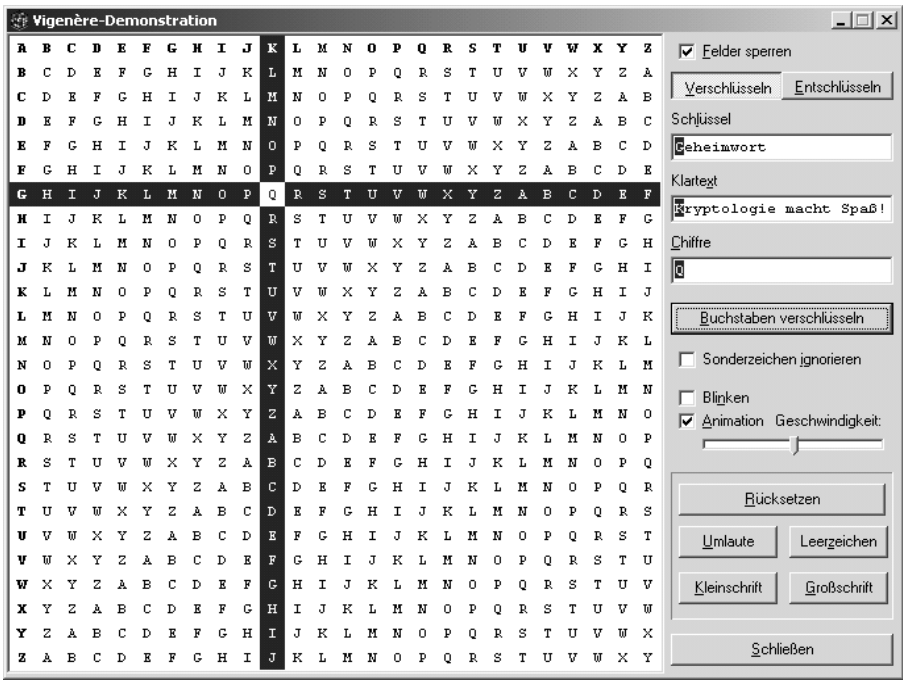
In einem zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler versuchen, eine Nachricht ohne Kenntnis des Schlüssels zu entschlüsseln. Hier werden sie erfahren, dass mit dem Caesar-Verfahren verschlüsselte Nachrichten sich durch Ausprobieren aller möglichen 25 Abstände mit vertretbarem Aufwand knacken lassen.

Anschließend sollte unter Einsatz des Werkzeugs *Krypto 1.5* von Michael Kühn gezeigt werden, wie das Ausprobieren verschiedener Schlüssel mithilfe des Computers drastisch beschleunigt wird.

Polyalphabetische Kryptographie – Vigenère

Die Erfahrung, dass auch ein beliebiger monoalphabetischer Substitutionscode durch eine Häufigkeitsanalyse geknackt werden kann, führte zu der Idee von Blaise de Vigenère, die Zeichen eines Textes abwechselnd mit verschiedenen Abständen von Geheimtextalphabet und Klartextalphabet zu verschlüsseln. Ein Schlüsselwort bestimmt, mit welchem Geheimtextalphabet ein Zeichen an einer bestimmten Position im Klartext verschlüsselt wird. Insgesamt werden so viele Geheimtextalphabete verwendet, wie das Schlüsselwort verschiedene Zeichen enthält; es handelt sich also um ein polyalphabetisches Verfahren.

Abbildung 9:
Anschauliche Animation des Vigenère-Verfahrens mit Krypto 1.5.



Das Werkzeug *Krypto 1.5* bietet eine sehr anschauliche Animation des Vigenère-Verfahrens. Die Schülerinnen und Schüler werden aufgefordert, eine Nachricht, die sie per E-Mail verschicken wollen, mit *Krypto* zu verschlüsseln und dabei die Animation zu beobachten, um das Vorgehen zu erklären. Das Verfahren wurde über 300 Jahre als sicher angesehen.

Mit dem Werkzeug *CrypTool* lässt sich zeigen, dass auch diese Verschlüsselung geknackt werden kann. So könnte die Lehrkraft eine mit Vigenère verschlüsselte E-Mail mit einem spannenden Betreff an alle Schülerinnen und Schüler senden, die offenbar aus Versehen an sie gelangte. Die Schülerinnen und Schüler wollen natürlich die Nachricht entschlüsseln und werden in diesem Moment auf die Möglichkeit aufmerksam gemacht, mit *CrypTool* die Chiffre zu knacken.

Aus dieser statistischen Angriffsmöglichkeit ergibt sich die Schlussfolgerung, dass bei einer sicheren Verschlüsselung mit dem Vigenère-Verfahren das Schlüsselwort eine Länge haben sollte, die größer als die der zu verschlüsselnden Nachricht ist. Außerdem sollte das Schlüsselwort selbst kein natürlichsprachliches Wort, sondern eine zufällig erzeugte Zeichenfolge sein, die jeweils nur ein einziges Mal eingesetzt werden darf. Das One-Time-Pad verhindert – wenn es korrekt angewendet wird – somit Angriffe auf die Verschlüsselung mittels statistischer Verfahren. Die Schwachstelle des Verfahrens liegt jedoch in der Übermittlung des Schlüssels. Die Beseitigung dieser Angriffsmöglichkeit wird durch asymmetrische Verschlüsselungsverfahren ermöglicht, die in den folgenden Stunden des Lernabschnitts behandelt werden.

Trennung von Ver- und Entschlüsseln 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 leicht geschieht, 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 aufwendig. Mit diesem Hilfsmittel entdecken die Lernenden den Diffie-Hellman-Schlüsseltausch. Eine ausführliche Beschreibung dieses Einstiegs in die asymmetrische Kommunikation findet sich in den Materialien.

Das Prinzip der asymmetrischen Kryptologie

Die Schülerinnen und Schüler erarbeiten mit der Animation »Vertraulichkeit und Authentizität durch asymmetrische Kryptologie herstellen« selbstständig das Prinzip der asymmetrischen Kryptographie im E-Mail-Kontext. (Die Animation steht kostenfrei zur Verfügung; siehe Anmerkung auf Seite 17.)

Dabei lernen sie die Funktion von öffentlichem und privatem Schlüssel kennen. In der Animation wird der geheime Schlüssel durch einen kleinen Tresor symbolisiert; der Inhalt ist immer nur für denjenigen sichtbar, der gerade die Rolle von Alice bzw. Bob einnimmt. Der öffentliche Schlüssel wird durch eine kleine Webseite dargestellt. Die Weltkugel 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.

Diese Stunde legt die Grundlage für die Beschäftigung mit RSA, während der eigentliche Verschlüsselungsvorgang hier noch als »Black-Box« funktioniert. Außerdem ist zu beachten, dass die verwendeten Schlüssel für eine sichere Kommunikation viel

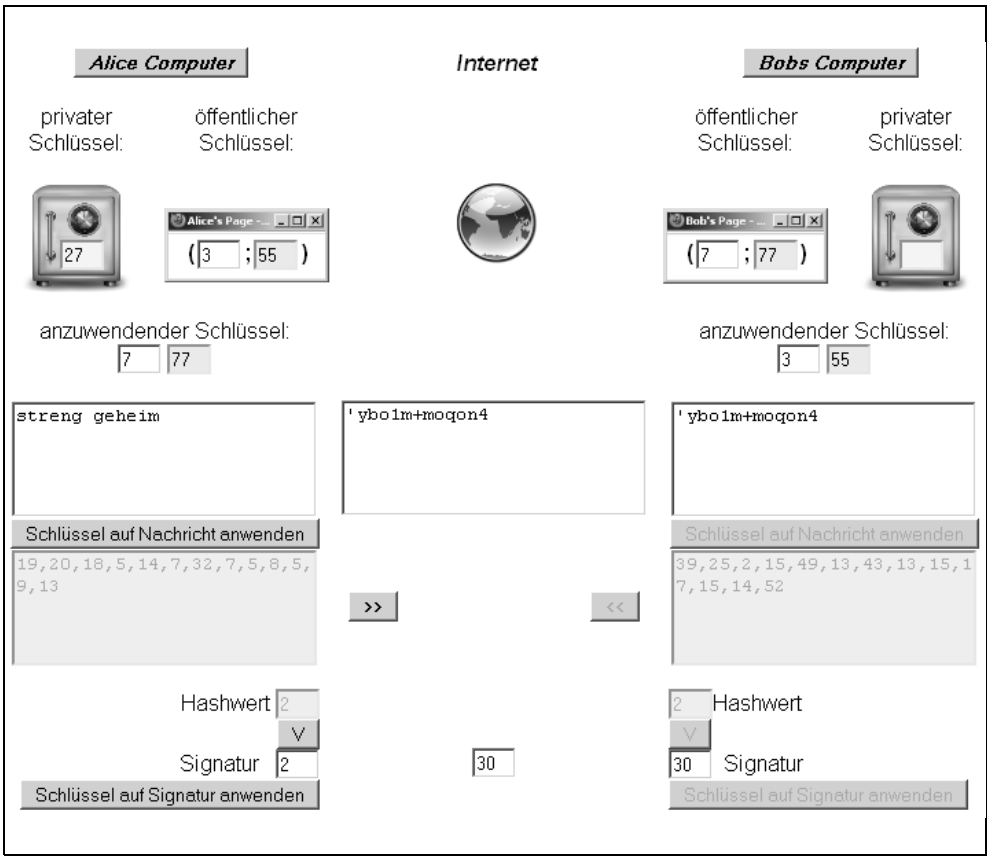


Abbildung 10:
Animation »Vertraulichkeit und Authentizität durch asymmetrische Kryptologie herstellen«.

Weiterführendes

Sollte ein revolutionär neues und effizientes Verfahren zur Primzahlfaktorisierung gefunden werden, würde aber auch die Verlängerung der Schlüssel nicht helfen. Dieses Szenario bildet die Grundlage für den Film »Sneakers« (vgl. 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.

zu klein sind. Informationen über die erforderlichen Schlüsselgrößen erhalten die Lernenden im weiteren Verlauf der Unterrichtsreihe.

Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und Zerlegung in Primfaktoren

In den vorangegangenen Stunden haben die Schülerinnen und Schüler bereits ein Beispiel für eine Falltürfunktion kennengelernt: das Vorhängeschloss. Für die asymmetrische Verschlüsselung ist aber eine andere Falltürfunktion von Interesse: die Primzahlfaktorisierung. Es ist zwar einfach, ein 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 zunutze: 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 zurzeit üblichen Schlüsselgrößen (mindestens 1024 Bit) unmöglich, aus diesem Produkt auf die Primfaktoren zu schließen. Solche Produkte aus genau zwei verschiedenen Primzahlen werden *Semiprimzahlen* genannt.

1024-Bit-Verschlüsselungen werden jedoch bald als nicht mehr sicher gelten. 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.

Für das Verständnis des später in diesem Lernabschnitt 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 Primzahlen und Semiprimzahlen erläutert, und es wird ein Verfahren eingeführt, das das Auffinden von Primzahlen ermöglicht (Sieb des Eratosthenes; *Anmerkung:* 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.).

Anschließend sollen die Schülerinnen und Schüler Semiprimzahlen in ihre Faktoren zerlegen, wobei sie erkennen, dass mit steigender Größe der zu untersuchenden Zahl der Aufwand der Faktorisierung immer höher wird – und irgendwann so groß ist, dass die Faktorisierung auch mithilfe eines Rechners nicht mehr durchzuführen ist.

Abbildung 11:
Ein Arbeitsbogen führt schrittweise in die Konstruktion eines Schlüsselpaars ein (hier mit eingetragener Lösung für die Primzahlen 5 und 11).

Das RSA-Verfahren – Lösung für p=5, q=11

Das RSA-Verfahren wurde 1978 von Rivest, Shamir und Adleman entwickelt.

1. Geeignete Schlüssel wählen

- Wähle zwei Primzahlen p und q!

  p = 5 und q = 11

- Berechne das Produkt N der beiden gewählten Primzahlen p und q!

  N = p · q = 5 · 11 = 55

- Berechne das folgende Produkt phi = (p-1)·(q-1)!

  phi = (5 -1)·(11 -1) = (4)·(10) = 40

- Bestimme zwei natürliche Zahlen d und e so, dass gilt: $(d \cdot e) \bmod phi = 1$
  (Für Interessierte: da der Rest der Division (d · e) : phi den Wert 1 ergibt sind die Zahlen d und e „modular invers" bezüglich der Division durch phi).

  erster Versuch:

  - Die erste Zahl, die als Rest einer Division durch 40 den Rest 1 lässt, ist 41:
    41 mod 40 = 1 — 41 lässt sich nicht in zwei Faktoren zerlegen, weil sie eine Primzahl ist.
    -> es gibt kein Zahlenpaar (d;e) mit d_e = 41

  zweiter Versuch:

  - Die zweite Zahl, die als Rest einer Division durch 40 den Rest 1 lässt, ist 81:
    81 mod 40 = 1 — 81 lässt sich als 3 _ 27 darstellen. Damit ist ein Zahlenpaar (d;e) mit d_e = 81 gefunden.

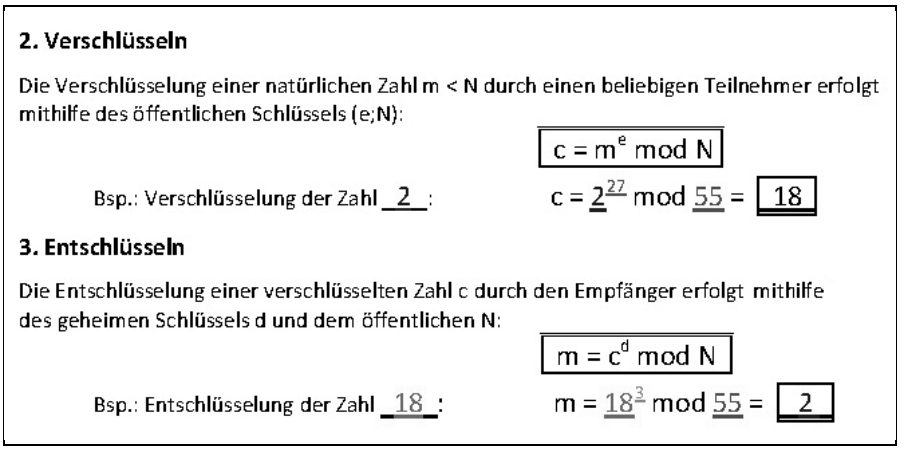
Nun sind ein **geheimer Schlüssel d** und ein **öffentlicher Schlüssel (e;N)** gefunden.

Implementierung asymmetrischer Kryptologie in RSA

Das 1978 entwickelte RSA-Verfahren ist ein asymmetrisches Verschlüsselungsverfahren, das genügend große Semiprimzahlen nutzt, um die nötige Sicherheit des Verfahrens zu gewähr-

leisten (zurzeit mindestens 1024 Bit). Die unter dem Gesichtspunkt der Sicherheit wichtigsten Grundlagen des Verfahrens haben die Schülerinnen und Schüler bereits in der Stunde »Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und die Zerlegung in Primfaktoren« kennengelernt.

Da das RSA-Verfahren für Schülerinnen und Schüler 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 Lernenden in diese für sie ungewohnte Rechenart ein (siehe Abb. 12).



2. Verschlüsseln

Die Verschlüsselung einer natürlichen Zahl m < N durch einen beliebigen Teilnehmer erfolgt mithilfe des öffentlichen Schlüssels (e;N):

$c = m^e \bmod N$

Bsp.: Verschlüsselung der Zahl 2 : $c = 2^{27} \bmod 55 = 18$

3. Entschlüsseln

Die Entschlüsselung einer verschlüsselten Zahl c durch den Empfänger erfolgt mithilfe des geheimen Schlüssels d und dem öffentlichen N:

$m = c^d \bmod N$

Bsp.: Entschlüsselung der Zahl 18 : $m = 18^3 \bmod 55 = 2$

Abbildung 12:
Auszug aus einem Arbeitsbogen zum Ver- und Entschlüsseln mithilfe eines öffentlichen und geheimen Schlüssels.

Anschließend soll das Verfahren angewendet werden – auch hierbei wird in dieser Doppelstunde 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 entschlüsselt.

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 entscheidenden 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 Chiffre zu knacken. Zu diesem Zweck können einige Schülerinnen und Schüler (oder alle – je nach Größe des Kurses) eine Chiffre zur Verfügung stellen. Gemeinsam versucht die Lerngruppe, den Modul 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. Mit dem gefundenen Schlüssel kann nun die Chiffre geknackt werden!

Sicherheit von RSA

Nachdem die Schülerinnen und Schüler in der letzten Doppelstunde erfahren haben, dass die händische Anwendung des RSA-Verfahren wegen der notwendigerweise sehr kleinen Schlüsselgrößen sehr unsicher ist, ist es naheliegend, 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 Schülerinnen und Schülern mithilfe von *CrypTool* (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 wir 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.

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* nicht mehr in vernünftiger Zeit geknackt werden.

4 Integrität der Nachricht und Authentizität des Absenders mit digitaler Unterschrift prüfen

Nachdem in den vorangegangenen Stunden die Frage beantwortet wurde, wie mittels Verschlüsselung Vertraulichkeit bei der E-Mail-Kommunikation hergestellt werden kann, steht im vorletzten Lernabschnitt der Unterrichtseinheit 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. Die damit erstellten Nachrichten werden – wie bereits in den Stunden 2 und 3 – mittels *SocketSniff* analysiert, um den Unterschied zu unverschlüsselten E-Mails zu verdeutlichen.

Mit dem Ende dieses Lernabschnitts haben die Schülerinnen und Schüler 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.

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« 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 sogenannte 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. Die andere Methode ist die Einbindung in ein »Web of Trust«. Hier bürgen jeweils Dritte für die Identität eines weiteren Teilneh-

mers im »Web of Trust«. Dadurch entsteht eine netzartige Struktur, in der jeder Teilnehmer für die Korrektheit einer bestimmten Anzahl von öffentlichen Signaturen bürgen kann.

Bezug zu den Bildungsstandards

Die Schülerinnen und Schüler …
- ▷ verstehen die Grundlagen des Aufbaus von Informatiksystemen und deren Funktionsweise und wenden diese zielgerichtet an.
- ▷ reagieren angemessen auf Risiken bei der Nutzung von Informatiksystemen (Prinzip der digitalen Unterschrift).

Das Prinzip der digitalen Unterschrift entdecken

In der ersten Stunde dieses Abschnitts beantworten die Schülerinnen und Schüler die Frage nach der Sicherstellung von Authentizität und Integrität bei der E-Mail-Kommunikation. Zu diesem Zweck arbeiten die Schülerinnen und Schüler mit der (erweiterten) Animation, die bereits bekannt ist. Anhand der Animation und der Erläuterung auf dem Arbeitsbogen, sind die Schülerinnen und Schüler in der Lage, die Funktionsweise der »digitalen Signatur« zu entdecken. Dabei lernen sie ebenfalls Hashfunktionen kennen und können in Grundzügen erläutern, wie diese funktionieren. Nachdem die Schülerinnen und Schüler das Verfahren durchdrungen haben, wird die Schrittfolge beim Versenden einer verschlüsselten und signierten E-Mail festgehalten.

Es fällt jedoch auf, dass lediglich der Inhalt der E-Mail verschlüsselt wird; die Kommunikation mit dem E-Mail-Server erfolgt nach wie vor unverschlüsselt. Ohne Angaben wie Empfänger und Absender kann eine E-Mail auch vom E-Mail-Server gar nicht zugestellt werden. Um diese Informationen jedoch vor unbefugtem Mitlesen (oder gar Manipulieren) auf dem Transportweg zu schützen, sollte zusätzlich zum Verschlüsseln der E-Mails selbst auch der Kommunikationskanal verschlüsselt werden. Etliche E-Mail-Provider bieten deshalb an, ihre E-Mail-Server über Verbindungen zu nutzen, die mit ***S**ecure **S**ockets **L**ayer* (SSL) bzw. ***T**ransport **L**ayer **S**ecurity* (TLS) verschlüsselt sind.

Digitale Unterschrift anwenden

Nachdem sich die Lernenden die theoretischen Grundlagen der asymmetrischen Verschlüsselung erarbeitet haben, sollen sie sich nun in der praktischen Anwendung dieses Verfahrens üben. Am Ende des Lernabschnitts sollen alle Schülerinnen und Schüler wissen, wie sie selbstständig ein Schlüsselpaar erstellen und wie sie die Verschlüsselung in E-Mail-Programmen (z.B. Thunderbird oder Outlook) einsetzen können.

Der erste Schritt der Unterrichtsstunde besteht darin, Schlüsselpaare mittels *OpenPGP* (bzw. *PGP4win* für Outlook) zu erzeugen und zu verwalten, oder alternativ ein (leider zeitlich begrenztes) Zertifikat über ein Trustcenter anzufordern. Mit diesem Schlüsselpaar allein ist das Verschlüsseln von Mails noch nicht zu bewerkstelligen. Zunächst muss dem E-Mail-Programm »beigebracht« werden, Verschlüsselung zu nutzen. Im Falle von Thunderbird sollte dafür das *Enigmail*-Plugin installiert werden, für Outlook-Benutzer reicht das oben genannte Paket *PGP4win*.

Anschließend tauschen die Schülerinnen und Schüler ihre öffentlichen Schlüssel aus und verwalten diese im E-Mail-Programm. Dadurch bilden sie ein »Web of Trust«. Die Schülerinnen und Schüler verschicken und empfangen nun (über den bekannten *Hamster*-Server) verschlüsselte und signierte E-Mails ihrer Mitschülerinnen. Um sich wirklich davon zu überzeugen, dass die erarbeiteten Anforderungen an sichere Kommunikation erreicht worden sind, erhalten die Schülerinnen und Schüler wieder den Auftrag, den aus- und eingehenden E-Mail-Verkehr mittels *SocketSniff* zu analysieren. Dabei werden sie erkennen, dass die Informationen der E-Mail nicht länger im Klartextformat verschickt werden. Damit hat die Lerngruppe – für sie nachvollziehbar – das Ziel erreicht, Authentizität, Integrität und Vertraulichkeit bei der E-Mail-Kommunikation herzustellen, und die Schülerinnen und Schüler sind in der Lage, ein solches System auf schulfremden PCs zu installieren.

PGP4win ist z.B. kostenfrei als »GNU Privacy Guard for Windows« (Gpg4win) erhältlich bei http://www.gpg4win.de/index.html

5

Warum sollte ich sicher kommunizieren?

Auf die Frage, warum man sicher kommunizieren sollte, bekommt man häufig die Antwort: »Ich habe doch nichts zu verbergen!« Die Antwort mag in den meisten Fällen sogar zutreffend sein. Doch wer hat nicht schon einmal seine Telefonnummer, seine Adresse oder sogar seine Bankverbindung unverschlüsselt übers Netz geschickt (man denke z. B. an Reisekostenabrechnungen)? Man würde vermutlich nie auf die Idee kommen, solch sensible Daten auf eine Postkarte zu schreiben – was im Wesentlichen der Kommunikation per E-Mail entspricht. Trotzdem herrscht beim System E-Mail ein leichtfertiger Umgang, der meist auf der Unwissenheit über die dabei entstehenden Gefahren basiert. Und selbst wenn man sich entscheidet, sicher mit den eigenen E-Mails umzugehen, fehlt häufig beim Kommunikationspartner die nötige Infrastruktur, um das eigene Vorgehen umzusetzen. Entscheidend ist also zu erkennen, welche Informationen einer sicheren Kommunikation bedürfen. Als Faustregel gilt hier: Ich sollte nichts in eine unverschlüsselte E-Mail schreiben, das ich nicht auch auf eine Postkarte schreiben würde.

Verlässt man das Feld der privaten und betrachtet die wirtschaftliche Kommunikation, so muss man die Anforderungen an die E-Mail-Sicherheit wesentlich höher ansetzen. Als zukünftige Mitglieder und Entscheidungsträger der Wirtschaftswelt müssen die Schülerinnen und Schüler erkennen, dass sicherer E-Mail-Verkehr in Unternehmen unbedingt notwendig ist. Die Kommunikation zwischen und innerhalb von Unternehmen ist weitaus sensibler, da sie als Angriffsziel dem potenziellen Hacker einen größeren monetären Gewinn verspricht.

Dass es sich hierbei nicht um Paranoia, sondern um handfeste Gefahren handelt, erkennt man an den Empfehlungen des Europäischen Parlaments: Da große Unternehmen mittlerweile ausgefeilte Sicherungssysteme und Richtlinien bezüglich ihrer Kommunikation besitzen, geraten vor allem kleine und mittelständische Unternehmen ohne entsprechendes Know-how ins Visier von Angreifern. Daraus folge, dass diese Betriebe verstärkt auf die Sicherheit ihrer Nachrichtenübermittlung achtgeben müssen (vgl. Europäisches Parlament, 2001). Aus der Empfehlung des Europäischen Parlaments ergibt sich die Frage, wer eine solche Sensibilisierung herbeiführen kann. Da die Sicherheit elektronischer Kommunikation unserer Ansicht nach ein Kerngebiet der Informatik ist, muss diese Aufgabe vor allem dem Informatikunterricht zufallen.

Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten […] Eine Zensur findet nicht statt.

GG Art. 5 Abs. 1

Bezug zu den Bildungsstandards

Die Schülerinnen und Schüler …
- ▷ benennen Wechselwirkungen zwischen Informatiksystemen und ihrer gesellschaftlichen Einbettung.
- ▷ nehmen Entscheidungsfreiheiten im Umgang mit Informatiksystemen wahr und handeln in Übereinstimmung mit gesellschaftlichen Normen.
- ▷ begründen Entscheidungen bei der Nutzung von Informatiksystemen.
- ▷ kommunizieren fachgerecht über informatische Sachverhalte.

Gruppenpuzzle zur Kommunikationsfreiheit

In diesem letzten Abschnitt der Unterrichtseinheit sollen die Schülerinnen und Schüler die Einsicht gewinnen, dass sichere E-Mail-Kommunikation nichts mit Sicherheitswahn zu tun hat, sondern eine sinnvolle Maßnahme ist, sich gegen kriminelle Aktivitäten präventiv zu schützen. Um dies zu bewerkstelligen, müssen die Schülerinnen und Schüler zunächst identifizieren, wer ein Interesse daran hat, Kommunikation abzuhören und welche Intentionen diese Akteure besitzen.

Dabei sollen sie auch erfahren, welchen Wert das Recht auf freie Kommunikation überhaupt darstellt: Kommunikationsfreiheit darf nicht als selbstverständliches Gut wahrgenommen werden. Weiterhin muss auch auf die Gefahr der Nutzung von Verschlüsselungssystemen hingewiesen werden: Wer z. B. in

Freiheit. Ich verstehe das Wort nicht, weil ich sie nie entbehren musste.

Jonas T. Bengtsson: Die Hölle ist, mit sich allein zu sein.
(Young Euro Connect, 2006)

China eine nichtstaatlich freigegebene Verschlüsselung benutzt, der macht sich bereits strafbar, und selbst in den USA wurde der Export von Verschlüsselungssystemen lange Zeit als Waffenexport angesehen (man betrachte den Fall »PGP«). Dies führt zu der Frage, welches Interesse Staaten besitzen könnten, Kommunikation abzuhören und protokollieren. Hier sei jedoch gleich erwähnt, dass Staaten sehr wohl ein gerechtfertigtes Interesse daran haben können, Kommunikation zu kontrollieren – und zwar genau dann, wenn es der Kriminalitätsbekämpfung und Gefahrenabwehr dient. Entscheidend ist dabei, dass es staatliche Kontrollstrukturen gibt, die den Missbrauch (z. B. Industriespionage) durch eigene staatliche Strukturen verhindern.

Anhand der jüngsten Ereignisse in der arabischen Welt können die Schülerinnen und Schüler erfahren, was es bedeutet, wenn ein Staat versucht, elektronische Kommunikation zu unterbinden. Dabei steht nicht nur die Frage im Vordergrund, wie so etwas konkret technisch durchgesetzt wird, sondern auch, was es für die Menschen bedeutet, elektronisch zu kommunizieren, welche politische Funktion diese Kommunikation besitzt und welche harten Konsequenzen die Kommunizierenden ertragen müssen. So trägt dieser letzte Lernabschnitt zur Erziehung der Schülerinnen und Schüler zu mündigen Bürgerinnen und Bürgern bei, indem diese den Nutzen von E-Mail-Sicherheit und den Wert von Kommunikationsfreiheit erkennen.

Zu diesem Zweck werden folgende Themen in einem Gruppenpuzzle arbeitsteilig erarbeitet und anschließend einander vorgestellt:

Das Themengebiet *Kommunikationsfreiheit* eröffnet die Frage, wie und warum Staaten E-Mail-Verkehr kontrollieren können. Anhand von Karikaturen und spannenden Fallbeispielen zu den jüngsten politischen Ereignissen erfahren die Schülerinnen und Schüler, was es bedeutet, ungehindert kommunizieren zu dürfen und was es heißt, diese Freiheit nicht zu besitzen.

Viele undemokratische Regime überwachen elektronische Kommunikation, um Dissidenten aufzuspüren und politische Proteste zu verhindern.

Das *Echelon-System* ist ein weltumspannendes Abhörsystem, das hauptsächlich zum Abfangen von Satellitenkommunikation dient. Die Beschäftigung mit Echelon ermöglicht den Schülerinnen und Schülern, eine Perspektive auf das Thema »Geheimdienste und Spionage« einzunehmen, die der Realität gerecht wird und die den das Thema umrankenden Mythos entzaubert. Dabei steht die Frage im Vordergrund, wer überhaupt ein Interesse daran hat, Kommunikation abzuhören, wie dies technisch umgesetzt wird und wie sich die Betroffenen davor schützen können.

De-Mail ist Bestandteil des sogenannten Online-Bürgerportals und soll als sichere Kommunikationsstruktur zwischen Bürgern, Behörden, Banken, Versicherungen und Privatfirmen dienen und den Brief als rechtskräftiges Kommunikationsmittel um die Vorzüge von E-Mail ergänzen. Die Entwicklung und Inbetriebnahme des Systems hat zu Diskussionen rund um das Thema Kommunikationssicherheit geführt, indem von Experten die Unzulänglichkeiten des Systems aufgezeigt wurden. Die Schülerinnen und Schüler entdecken dabei die Funktionsweise des Systems und erfahren gleichzeitig anhand des Streits über das Bürgerportal, welche Auswirkungen ein solches Informatiksystem auf unsere Gesellschaft haben kann.

Pretty Good Privacy (PGP) ist ein weit verbreitetes freies Verschlüsselungssystem, dessen Historie sich wie ein Kriminalroman liest. Der Export des Systems aus den USA wurde lange Zeit durch die US-Regierung als Waffenhandel interpretiert. Das Exportverbot wurde umgangen, indem der Quellcode des Programms in Buchform gedruckt und von freiwilligen Helfern in aller Welt per Hand abgeschrieben wurde. Neben einer bewegten Geschichte bietet PGP den Schülerinnen und Schülern die Möglichkeit, ein aktuelles System kennenzulernen, das – bis heute – Standards in Sachen Verschlüsselung gesetzt hat.

Unter http://www.informatik-im-kontext.de/ sind beim Stichwort »Email nur für Dich« alle Lernabschnitte mit einer einführenden Sachanalyse, einem Vorschlag für eine Verlaufsplanung und einer ausführlichen Beschreibung der relevanten Materialien dokumentiert, wobei auch eine ZIP-Datei mit allen Dateien zum Herunterladen angeboten wird.

In dieser Unterrichtsreihe eingesetzte Software

Verschlüsselungsumgebung CrypTool 1.4.30:
http://cryptool.de/

Mozilla-Thunderbird-PGP-Add-On Enigmail:
https://addons.mozilla.org/de/thunderbird/addon/enigmail/

E-Mail-Server Hamster (Volkers Hamsterseiten):
http://hamster.volker-gringmuth.de/
(Hinweise zum Einrichten des E-Mail-Servers in der ausführlichen Dokumentation der Reihe beachten! Administrator-Rechte erforderlich!)

OpenPGP-Implementierung GnuPG:
http://www.gnupg.org/download/index.de.html#auto-ref-2

Verschlüsselungsumgebung Krypto 1.5:
http://www.kuehnsoft.de/krypto.php

E-Mail-Client Mozilla Thunderbird:
https://www.mozilla.org/de/thunderbird/

Netwerkanalysewerkzeug SocketSniff:
http://www.nirsoft.net/utils/socket_sniffer.html

Netwerkanalysewerkzeug Wireshark:
http://wireshark.org/

Literatur und Internetquellen

AKBSI – Arbeitskreis »Bildungsstandards« der Gesellschaft für Informatik (Hrsg.): Grundsätze und Standards für die Informatik in der Schule – Bildungsstandards Informatik für die Sekundarstufe I. Empfehlungen der Gesellschaft für Informatik e.V. vom 24. Januar 2008. In: LOG IN, 28. Jg. (2008), Heft 150/151, Beilage.
http://www.informatikstandards.de/

Breier, N.; Hilger, S.; Lange, N.; Schulz, J.: Mein Computer spricht mit mir – Kontextbezogene Unterrichtseinheit zur Mensch-Maschine-Kommunikation mittels gesprochener Sprache. In: LOG IN, 28. Jg. (2008), Heft 154/155, S. 61–67.

BVerfG – Bundesverfassungsgericht: 2 BvR 2233/07 vom 18.5.2009 – Verfassungsbeschwerden gegen § 202c Abs. 1 Nr. 2 StGB in Verbindung mit § 202a StGB in der Fassung des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 7. August 2007.
http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html

Engbring, D.; Pasternak, A.: Einige Anmerkungen zum Begriff IniK. In: I. Diethelm; Chr. Dörge; C. Hildebrandt; C. Schulte (Hrsg.): Didaktik der Informatik – Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik. 6. Workshop der GI-Fachgruppe DDI. Reihe »GI-Edition LNI – Lecture Notes in Informatics«, Band P-168. Bonn: Köllen Verlag, 2010, S. 119–124.
http://medienwissenschaft.uni-bayreuth.de/inik/material/inik_kurz4.pdf

Europäisches Parlament (Hrsg.): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschafliche Kommunikation (Abhörsystem ECHELON). Drucksache A5-0264/2001, Teil 1, Berichterstatter: Gerhard Schmid. 11. Juli 2001.
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE

Freischlad, St.; Stechert, P.: FILIUS – Internetworking für den Informatikunterricht. Siegen: Universität Siegen, 2003.

Gramm, A.: Rollenspiel »Wie funktioniert das Internet?«, 2009.
http://informatik.schule.de/material/rollenspiel__internet.zip

Koubek, J.; Schulte, C.; Schulze, P.; Witten, H.: Informatik im Kontext (IniK) – Ein integratives Unterrichtskonzept für den Informatikunterricht. In: B. Koerber (Hrsg.): Zukunft braucht Herkunft – 25 Jahre »INFOS – Informatik und Schule«. INFOS 2009 – 13. GI-Fachtagung Informatik und Schule 21.–24. September 2009 in Berlin. Reihe »GI-Edition LNI – Lecture Notes in Informatics«, Band P-156. Bonn: Köllen Verlag, 2009, S. 268–279.
http://medienwissenschaft.uni-bayreuth.de/inik/material/InformatikImKontextINFOS2009.pdf

Koubek, J. u. v. a.: Informatik im Kontext – IniK für alle, 2011.
http://www.informatik-im-kontext.de/

mpfs – Medienpädagogischer Forschungsverbund Südwest (Hrsg.): JIM-Studie 2010 – Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger. Stuttgart: Medienpädagogischer Forschungsverbund Südwest, 2010.
http://www.mpfs.de/fileadmin/JIM-pdf10/JIM2010.pdf

wdr – Westdeutscher Rundfunk: Sachgeschichten – Folge »Internet«, o. J.
http://www.wdrmaus.de/sachgeschichten/sachgeschichten/sachgeschichte.php5?id=84

Witten, H.; Hornung, M.: Chatbots. – Teil 1: Einführung in eine Unterrichtsreihe zu »Informatik im Kontext« (IniK). In: LOG IN, 28. Jg. (2008), Heft 154/155, S. 51–60. – Teil 2: Der Turing-Test und die Folgen. In: LOG IN, 29. Jg. (2009), Heft 157/158, S. 63–74.

Alle Internetquellen wurden zuletzt am 31. Oktober 2011 geprüft.

Beilage zu LOG IN, 31 Jg. (2011), Heft Nr. 169/170

Das Projekt *Informatik im Kontext*
wird gefördert von der

Senatsverwaltung für Bildung,
Wissenschaft und Forschung Berlin
Otto-Braun-Straße 27
10178 Berlin
URL: http://www.berlin.de/sen/bwf/

LOG IN Verlag GmbH
Redaktion LOG IN
Friedrichshaller Straße 41
14199 Berlin
E-Mail: redaktionspost@log-in-verlag.de
URL: http://www.log-in-verlag.de/


LOG IN
VERLAG