

E-Mail (nur?) für Dich - Beschreibung der Unterrichtsreihe

Vorbemerkungen zur Unterrichtsreihe

In der als 19-stündiger, kumulativer Lernprozess für Lerngruppen ab Klasse 10 angelegten Unterrichtsreihe „E-Mail (nur?) für Dich“ werden zunächst an dem lebensweltlichen Beispiel E-Mail Kenntnisse über die technische Realisierung privater Kommunikation über öffentliche Computernetzwerke erarbeitet. Dieses Wissen wird dann angewendet, um Gefahren des Mitlesens und Manipulierens von Nachrichten zu entdecken und zu bewerten und Möglichkeiten zur Herstellung von vertrauensbildenden Maßnahmen wie Verschlüsselungsverfahren und digitales Signieren zu beurteilen.

Dieses Vorgehen bietet gleich mehrere Vorteile: Durch die Thematisierung der von Schülerinnen und Schülern oft täglich genutzten Kommunikation über das Internet einerseits und dem Charakter von Knobelaufgaben beim Ver- und Entschlüsseln von Texten andererseits wird ein hohes Maß an Motivation erreicht. Mit der sinnstiftenden Verbindung von technischen Aspekten der Kommunikation mit der Kryptologie erfahren die Schülerinnen und Schüler, dass sie erworbenes Wissen in einer neuen Situation konstruktiv anwenden und dabei Wissen aus anderen Fachgebieten wie z.B. der Mathematik und der Geschichte gewinnbringend einbringen können. Darüber hinaus erscheint das Thema Kommunikation in hohem Maße gendergerecht. Auch heute gehört die gewählte Anwendung E-Mail neben sozialen Netzwerken und Instant Messengers zu den drei meist genutzten Kommunikationsmitteln, wobei sich Kommunikation als Zweck der Computernutzung in den letzten 12 Jahren von 34% auf 45% erhöhte und damit heute vor Informationsbeschaffung und Unterhaltung den größten Anteil verschiedener Nutzungen hat. Die Nutzung von E-Mail hat sich dabei von 20% auf 55% erhöht (vgl. dazu S.33 f. der Studie "Jugend, Information, (Multi-) Media 2009" (JIM 2009) des Medienpädagogischen Forschungsverbunds Südwest (MPFS): <http://www.mpfs.de/fileadmin/JIM-pdf09/JIM-Studie2009.pdf> sowie S. 40 f. der Studie "Jugend, Information, (Multi-) Media 1998" (JIM 1998) des MPFS: <http://www.mpfs.de/fileadmin/Studien/JIM1998.pdf>).

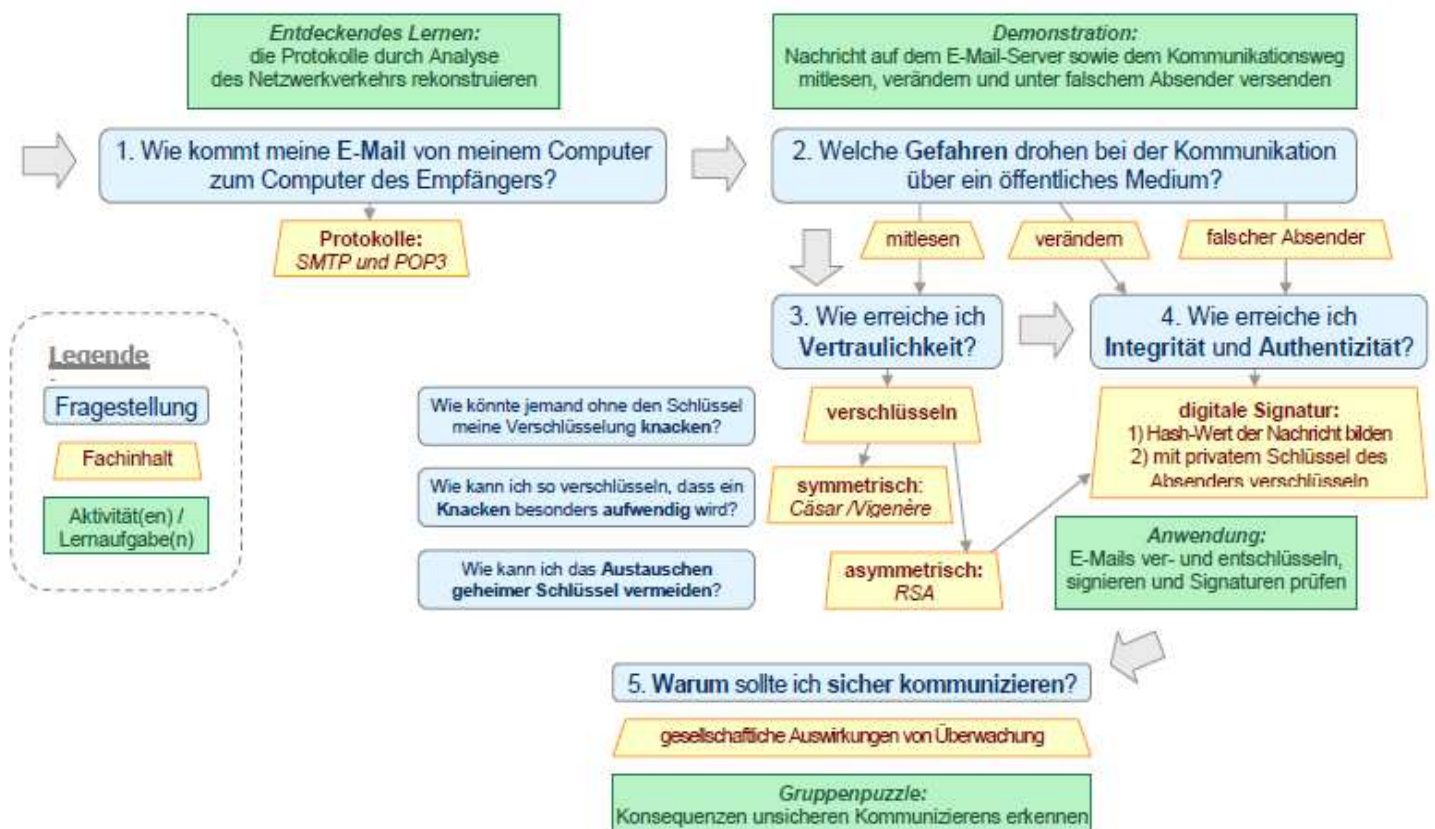
Die Reihe setzt das Prinzip von Informatik im Kontext ([informatik-im-kontext.de](http://www.informatik-im-kontext.de)) wie folgt um:

1. Mit dem Thema "Sichere Kommunikation über öffentliche Netzwerke" wurde ein vieldimensionaler Kontext gewählt. Dabei entstammt die erarbeitete Technologie E-Mail aus dem unmittelbaren Lebensumfeld von Schülerinnen und Schülern.
2. Es werden gezielt Kompetenzen aus verschiedenen der in den Bildungsstandards der GI (<http://www.informatikstandards.de>) beschriebenen Kompetenzbereichen gefördert. Dabei werden eine Vielzahl von Kompetenzbereichen berührt, 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.

Struktur der Unterrichtsreihe

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 bei 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 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 auf einander aufbauen, werden an einigen Stellen Anregungen für optionale, vertiefende Exkurse angeboten.

Einen Überblick über Fragestellungen, Themen und Lernformen der Reihe bietet folgende Graphik:



1. Wie kommt eine E-Mail von meinem Computer zum Computer des Empfängers? (3 Stunden)
2. Welche Gefahren bestehen bei der Kommunikation über öffentliche Medien? (2 Stunden)
3. Wie kann ich mit Verschlüsseln Vertraulichkeit herstellen? (10 Stunden)
4. Wie kann ich mit einer digitalen Unterschrift die Integrität der Nachricht und die Authentizität des Absenders überprüfen? (2 Stunden)
5. Warum sollte ich sicher Kommunizieren? (2 Stunden)

Notwendige Vorkenntnisse

Dies erfordert folgende Vorkenntnisse der Schülerinnen und Schüler:

- Jeder an das Internet angeschlossene Computer lässt sich über eine eindeutige **IP-Adresse** identifizieren.
- Nachrichten werden solange von einem Computer an Nachbarcomputer **weitergeleitet**, bis sie beim Computer des Empfängers der Nachricht eingetroffen ist.

Sollten die Schülerinnen und Schüler nicht über diese Vorkenntnisse verfügen, lassen sich diese z.B. mit folgenden Materialien vorab erarbeiten:

- Sachgeschichte der Sendung mit der Maus (WDR) zum Thema Internet:
<http://www.wdrmaus.de/sachgeschichten/sachgeschichten/sachgeschichte.php?id=84>
- Rollenspiel "Wie funktioniert das Internet?" (A. Gramm):
http://bildungsserver.berlin-brandenburg.de/fileadmin/bbb/unterricht/faecher/naturwissenschaften/informatik/technische_informatik/netze/rollenspiel_internet.zip
zur Einführung in HTML bietet sich folgende Übung an:
http://www.menzelschule.de/data/Uebung_Einfuehrung_in_HTML.zip (A. Gramm)
- Interaktive Lernumgebung *FILIUS*: <http://www.die.informatik.uni-siegen.de/pgfilius>
dazu passend:
 - [Anleitung mit Übungen](#)
 - Szenario [Vermittlungsrechner und DNS](#)
 - Szenario [E-Mail-Server und Clients](#)

Benötigte Software

Ein Teil der eingesetzten Software (Socket Sniff, Hamster) ist nur für die Windows-Plattform verfügbar (getestet mit Windows XP und Windows 7). Sollten Ihnen sinnvolle Alternativen für andere häufig eingesetzte Plattformen (Linux, Mac) bekannt sein, so freuen wir uns über einen Hinweis an:
gramm - at - menzelschule.de

Mozilla *Thunderbird* deutsche Version (<http://de.www.mozillamessaging.com/de/thunderbird/>)

Thunderbird-Add-On *Enigmail* (<https://addons.mozilla.org/de/thunderbird/addon/71/>)

OpenPGP (GnuPG) <http://www.gnupg.org/download/index.de.html#auto-ref-2>

(Link zum Windows-Installer: <ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.10b.exe>)

Socket Sniff (http://www.nirsoft.net/utils/socket_sniffer.html)

Wireshark (<http://wireshark.org>)

Krypto 1.5 (<http://www.kuehnsoft.de/krypto.php>),

(Link zum Download der ZIP-Datei: <http://www.kuehnsoft.de/download/krypto.zip>)

CrypTool 1.4.30 (stabile beta) (<http://cryptool.de>)

Hamster E-Mail-Server (<http://hamster.volker-gringmuth.de>)

(Link zum Download der ZIP-Datei: <ftp://hamster.ftp.fu-berlin.de/Hamster.23.4.zip>)

→ Der *Hamster*-Server muss mit Administrator-Rechten gestartet werden und benötigt darüber hinaus ggf. Administrator-Rechte um Firewall für Mail-Server freizuschalten!

→ *Krypto* 1.5 und *Socket Sniff* müssen nicht installiert werden,

dann aber in einem Gruppenverzeichnis für alle Teilnehmer erreichbar sein.

Beschreibung der Lernabschnitte und Materialien

Die Lernabschnitte und relevanten Materialien sind in den folgenden Abschnitten beschrieben. Dabei sind für jede Stunde Verlaufsplanung und Materialien angegeben. Die Verlaufsplanungen sind als *Empfehlungen* zu verstehen und erfordern eine Anpassung an Vorwissen und Arbeitsweise der konkreten Lerngruppen!

Wir empfehlen, alternativ zum Browsen der Dokumente am Computer sich sämtliche Arbeitsbögen und Verlaufsplanungen mit folgenden Dokumenten auszudrucken und je in einem Schnellhefter parallel zur Lektüre der Beschreibung der Lernabschnitte bereitzuhalten:

- [Verlaufsplanungen für sämtliche Stunden in einem PDF-Dokument](#) [19 Seiten]
- [Arbeitsbögen und Materialien für sämtliche Stunden in einem PDF-Dokument](#) [52 Seiten, ohne optionale Ergänzungen]

Bei Bedarf können Sie sich darüber hinaus sämtliche Materialien zur Reihe in einer Zip-Datei unter <http://www.informatik-im-kontext.de> herunterladen, die Sie bequem für den Unterricht auf Ihrem USB-Stick oder Ihrem Heimatverzeichnis entpacken können.

Lernabschnitt 1: Wie kommt eine E-Mail von meinem Computer auf den Computer des Empfängers? (3 Std.)

In entdeckendem Lernen erarbeiten Schülerinnen und Schüler in diesem Schritt das Konzept eines Kommunikationsprotokolls und lernen zwei typische Protokolle zum Versenden und Empfangen von E-Mails kennen. Am Anfang des Lernabschnitts sollen die Schülerinnen und Schüler nachvollziehen, warum ein Protokoll überhaupt für den Erfolg einer nonverbalen Kommunikation nötig ist. Um dies zu erreichen, wird auf einen Einstieg auf der technischen Ebene verzichtet.

Der erste Lernabschnitt legt zugleich die Grundlagen für die in der Unterrichtseinheit folgenden Inhalte: Wer Gefahren und Risiken von E-Mail-Kommunikation identifizieren will, der muss zunächst die technischen Abläufe verstehen, um mögliche Angriffspunkte erkennen zu können. Gleichzeitig bietet das Themenfeld „Protokolle“ die Möglichkeit, informationstechnische Konzepte wie etwa die Server-Client-Architektur zu behandeln.

Sachanalyse

Der Begriff des Protokolls in seiner heutigen Bedeutung gründet auf dem aus der diplomatischen Praxis bekannten Protokollen und meint zunächst nichts anderes als eine Sammlung von Regeln. Diese Regeln legen fest, wer wann auf welche Art und Weise zu agieren hat. Gegen die zweite Bedeutung des Begriffs – das Protokoll als Mitschrift – muss das Protokoll im Sinne einer Regelsammlung deutlich abgegrenzt werden.

Eine notwendige Voraussetzung für den Erfolg von Kommunikation zwischen Computern besteht in der Einhaltung dieser Regeln. Ein Rechner muss von seinem Gegenüber nicht nur auf Basis eines gemeinsamen Befehlssatzes verstanden werden, es ist auch notwendig festzulegen, wann wer etwas 'zu melden' hat. Um dies gewährleisten zu können, wurden für den Mailverkehr bereits in den 80er Jahren Kommunikationsprotokolle entwickelt, die seitdem stetig erweitert wurden.

In diesem Unterrichtsabschnitt stehen die Protokolle SMTP und POP3 im Fokus. Das SMTP (Simple Mail Transfer Protocol) dient zum Versenden und Weiterleiten von Nachrichten, das POP3 (Post Office Protocol) zum Abholen von Nachrichten. Die zwei Akteure der Kommunikation mittels POP3 und SMTP sind Server und Client. Beide Protokolle laufen auf ähnliche Art und Weise ab: Der Client öffnet

die Verbindung zum Server und authentifiziert sich. Anschließend sendet, bzw. liest der Client E-Mail-Nachrichten und meldet sich anschließend ab. Der Ablauf der Kommunikation auf Basis der Protokolle findet sich im Detail auf den Arbeitsbögen zu POP3 und SMTP (siehe Stunden 2/3).

Standardbezug

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.

Stunde 1: Regeln zur Kommunikation aufstellen – ein eigenes Protokoll entwerfen

Um Schülerinnen und Schülern für die Notwendigkeit der Festlegung und Einhaltung von Protokollen zu sensibilisieren bietet es sich an, ihnen folgenden Auftrag zu stellen:

*"Entwickelt ein Verfahren um mit einer unter einer Tür verlaufenden Schnur **ohne zu sprechen und ohne weitere Gegenstände** ein Wort zu kommunizieren! Ein/e Schüler/in auf der einen Seite der Tür wird nachher ein beliebiges Wort genannt bekommen, dass sie/er dann der Mitschülerin / dem Mitschüler auf der anderen Seite der Tür übermittelt."*

Als Hilfsmittel könnte z.B. der Morsecode oder eine durchnummerierte Aufstellung der Buchstaben des Alphabets bereitgestellt werden. Hilfen wie z.B. der Morsecode sind jedoch nicht zwingend notwendig und können als fakultatives Hilfsmittel für schwächere Gruppen 'in der Hinterhand' gehalten werden!

Der Ablauf des Unterrichts ist dabei dreigeteilt: zunächst entwickeln die Schülerinnen und Schüler in Kleingruppen ihre Kommunikationsregeln. Anschließend erhalten sie Zeit, diese Regeln zu testen und ggf. zu modifizieren. In der Auswertung können dann die Verfahren verschiedener Gruppen vor der gesamten Klasse vorgeführt und verglichen werden. Dabei können Aspekte wie Geschwindigkeit und Fehleranfälligkeit der Übertragung als Kriterien in die Betrachtung eingebracht werden und ggf. bereits erste Gemeinsamkeiten der Protokolle wie Startsignale, Bestätigungen, Fehlermeldungen als allgemeine Bestandteile vieler Protokolle dokumentiert werden und der Begriff des **Protokolls** als die "Regeln/Absprachen zur Kommunikation" definiert werden (in gezielter Abgrenzung zur Verwendung für "Bericht").

Material:

- Arbeitsbogen „Kommunikation ohne Worte - ein Kommunikationsprotokoll vereinbaren“ mit verschiedenen Übertragungs-codes als Hilfestellung

Stunden 2/3: SMTP- und POP3-Protokoll mit einem Netzwerkanalyse-Werkzeug erfassen und die Protokolle rekonstruieren

Durch die Analyse authentischen Netzwerkverkehrs entdecken die Schülerinnen und Schüler die E-Mail-Protokolle SMTP und POP3. Da in diesem Zusammenhang E-Mails und Passwörter sichtbar werden (siehe Abschnitt 2 zu Gefahren bei der Kommunikation über öffentliche Medien), 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, z.B. den *Hamster* von Volker Gringmuth, auf einem Rechner des Computerraums zu starten und dort Benutzerkonten für die Schülerinnen und

Schüler anzulegen, für die sie dann ihren E-Mail-Client (z. B. *Thunderbird*) auf den Schülerrechnern einrichten. Als Netzwerkanalyse-Werkzeug bietet sich z. B. *Socket Sniff* an (siehe Hinweis zu rechtlichen Aspekten des Einsatzes von Netzwerkanalyse-Werkzeugen zu Bildungszwecken unter „Software“).

Die Konfiguration des E-Mail-Postfachs mit *Thunderbird* sowie das Analysieren von Netzwerkverkehr mit *Socket Sniff* sind jeweils in einer Anleitung für die Hand der Schülerinnen und Schüler beschrieben. Ein alternativer Einsatz der didaktischen Simulations-Umgebung FILIUS wäre an dieser Stelle auch denkbar, erscheint aber weniger geeignet, um tatsächliche Gefahren an entfernten Geräten (z.B. "man-in-the-middle"-Angriff) realistisch erlebbar zu machen.

Die Schülerinnen und Schüler richten zunächst ihren E-Mail-Client ein und lassen sich dann vom Lehrer am E-Mail-Server ein Benutzerkonto einrichten. Von Beginn an wird vereinbart, dass als Benutzernamen die Vornamen der Schülerinnen und Schüler gelten, ggf. sind doppelt auftretende Namen oder Sonderzeichen individuell zu berücksichtigen. Beim Einrichten des Postfachs am Server (Menü im Hamster "Einstellungen >> Benutzerverwaltung und Passworte", dann Knopf "Neuer Nutzer") geben die Schülerinnen und Schüler ihr Passwort zweimal selbst ein (Knopf "Ändern" im oberen Bereich des Benutzer-Dialogs). Der Lehrer sollte hier zum einen demonstrativ wegschauen, zum anderen sollten die Schülerinnen und Schüler vor der Wahl des Passworts darauf hingewiesen werden, sich ein neues Passwort auszudenken und keines zu verwenden, das sie bereits nutzen. Auch bietet sich hier die Gelegenheit die Wahl sicherer Passwörter zu thematisieren, z.B. durch Bilden eines Akronymes über einem Satz, z.B. "Bin ich deine Nummer 1 ?" -> "BidN1?".

Durch zwei vorstrukturierte Arbeitsbögen gelenkt, erarbeiten die Schülerinnen und Schüler zunächst jeweils eines der beiden Protokolle in Partnerarbeit, wobei neben der Herstellung der korrekten Reihenfolge durch die Zuordnung sinnvoller Bezeichnungen für die einzelnen Schritte auch eine inhaltliche Interpretation der ausgetauschten Nachrichten gefordert wird.

In eine anschließenden Austauschphase vergleichen sie mit Experten für das jeweils andere Protokoll beide Protokolle und notieren Gemeinsamkeiten wie Begrüßung, Benutzerauthentifizierung, Versenden der E-Mail, Abmeldung.

Um zu überprüfen, ob die Protokolle richtig rekonstruiert wurden, kann die Musterlösung zum Vergleich angeboten werden. Alternativ oder optional additiv kann der Mailserver direkt über *Telnet* angesprochen werden und versucht werden, gemäß den rekonstruierten Protokollen eine E-Mail zu versenden oder E-Mails anzeigen zu lassen. Das Vorgehen ist in der Anleitung "Unterhaltung mit einem E-Mail-Server via Telnet" beschrieben. Die "freie" Kommunikation über Telnet ist für das POP3 Protokoll recht effizient, da hier schnell "echte" E-Mails in der ungewöhnlichen Darstellung der Eingabeaufforderung angezeigt werden. Das Versenden einer E-Mail erfordert dagegen vergleichsweise viele Eingaben und eine Base64-Kodierung von Benutzername und Passwort in SMTP, wobei das Übertragen der kodierten Zeichenketten in die Eingabeaufforderung fehleranfällig ist.

Material:

- Arbeitsbogen zu SMTP
 - Arbeitsbogen zu POP3
 - Musterlösung zu SMTP und POP3
 - Anleitung E-Mail-Client Thunderbird einrichten
- (Sie können die Anleitung für den Einsatz in Ihrem Computerraum anpassen, indem Sie die Bezeichnung "unsermailserver" durch den Rechnernamen Ihres E-Mail-Servers ersetzen:
- Anleitung als MS Word-Dokument, Suchen und Ersetzen mit "Strg + H"
 - Anleitung als OpenOffice.org Writer-Dokument, Suchen und Ersetzen mit "Strg + F" - die drei Einträge in den Textfeldern sind im OpenOffice jedoch per Hand zu ersetzen!

- Anleitung Netzwerkverkehr mit Socket Sniff analysieren
- Anleitung Unterhaltung mit einem E-Mail-Server via Telnet
- Webseite <http://decodebase64.com> zum Dekodieren von Base64-kodierten Texten

Software:

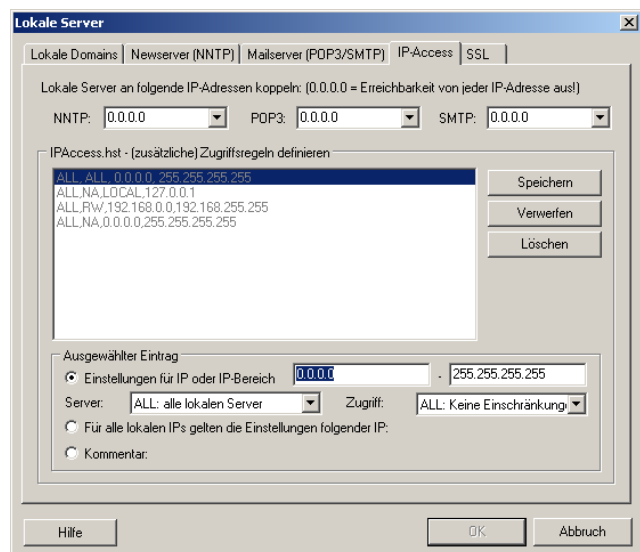
- **Thunderbird** - E-Mail-Client von Mozilla (falls nicht bereits installiert):
<http://de.www.mozillamessaging.com/de/thunderbird>
- **Socket Sniff** - Netzwerkanalyse-Werkzeug von Nir Sofer:
http://www.nirsoft.net/utils/socket_sniffer.html
Socket Sniff kann nach dem Entpacken ohne weitere Installation gestartet und somit auch z. B. über ein Tausch-Verzeichnis an die Schülerinnen und Schüler verteilt werden.
- **Hamster** - E-Mail-Server von Volker Gringmuth in der Version 1.3.23.4:
Download: <ftp://hamster.ftp.fu-berlin.de/Hamster.23.4.zip>
Hinweise und Informationen des Authors: <http://hamster.volker-gringmuth.de>

WICHTIGE HINWEISE zum Einrichten des E-Mail-Servers:

Keine Angst! Den E-Mail-Server "Hamster" im Schulnetz bereitzustellen ist nicht schwer, wenn folgende Hinweise beachtet werden: Der Hamster benötigt nach dem Entpacken keiner weiteren Installation. Das Starten des E-Mail-Servers erfordert jedoch **Administrator-Rechte**. Es wird empfohlen, das Programm **auf einen USB-Stick** zu entpacken und von dort unter einem Benutzerkonto mit Administrator-Rechten zu starten. So lässt sich auch verhindern, dass Schülerinnen und Schüler die E-Mail-Plattform außerhalb des Unterrichts weiter nutzen.

Der E-Mail-Server wird nach der Installation standardmäßig so gestartet, dass er gegen Anfragen von anderen Rechnern abgeschirmt ist. Soll der Server im Netzwerk verfügbar sein (und das soll er hier!) so sind **unbedingt** folgende **Einstellungen zu verändern**:

- Wählen Sie den Menüpunkt *Einstellungen >> Lokale Server*,
- dann das Registerblatt *IP-Access*.
- Eine sinnvolle Einstellung wäre, den Server nur für das lokale Netz freizugeben. Funktioniert das nicht, so lassen sich für die begrenzte Einsatzzeit des Servers Schreibrechte für alle IP-Adressen zwischen 0.0.0.0 und 255.255.255.255 gewähren:



Fällt die Verwendung eines Netzwerkanalysewerkzeugs nicht unter den Geltungsbereich von §202c StGB ("Hacker-Paragraph")?

Nein, es sei denn, es wird mit dem Vorsatz einer schadhafte Handlung eingesetzt, was in unserem Fall ausgeschlossen ist. Ein Hochschullehrer aus dem IT-Bereich hatte Verfassungsbeschwerde eingelegt, weil er sich in seiner Forschungs- und Lehrfreiheit eingeschränkt sah, da er mit seinen Studenten im Rahmen der Ausbildung auch Software zu Computersicherheit behandeln wollte. Das Bundesverfassungsgericht hat am 18.05.2009 die Verfassungsbeschwerde nicht angenommen und dies damit begründet, dass der Beschwerdeführer von dem Gesetz nicht betroffen sei, da der Einsatz

entsprechender Software ohne den Vorsatz des schadhafte Missbrauchs nicht strafbar sei. Die Notwendigkeit des Vorsatzes gehe zwar nicht aus dem Gesetzestext selbst, wohl aber aus einer EU-Richtlinie, die das Gesetz umsetzt, hervor. In der Anhörung des Gesetzes wurde darauf hingewiesen, dass die entsprechende Passage im Sinne der Richtlinie auszulegen sei, was das BVG mit der Ablehnung der Beschwerde tat.

Begründung der Ablehnung der Beschwerde durch das BVG zum Nachlesen:

http://www.bundesverfassungsgericht.de/entscheidungen/rk20090518_2bvr223307.html.

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. Portscannen auf Rechnern im Internet) eine strafbare Handlung darstellen kann. Unabhängig von der juristischen Lage sollte man sich als Pädagoge fragen, ob es sinnvoll ist, Schülerinnen und Schülern aktiv solche Werkzeuge anzubieten. Hier bietet *Socket Sniff* gegenüber anderen Netzwerkanalysewerkzeugen wie *Wireshark* den Vorteil, dass es nur solchen Netzwerkverkehr wiedergibt, der auch an eine auf dem Computer des Benutzers laufende Anwendung adressiert ist und so kein Mitlesen von Nachrichten erlaubt, die für andere Computer bestimmt sind.

Lernabschnitt 2: Welche Gefahren bestehen bei der Kommunikation über öffentliche Medien? (2h)

In diesem Lernabschnitt werden die Schülerinnen und Schüler in einer fiktiven Situation verschiedene reale Gefahren der Kommunikation im Internet erleben. Dazu senden sie sich – wie bereits im Lernschritt zur Rekonstruktion der Protokolle SMTP und POP3 – fiktive Nachrichten über einen auf dem Lehrerrechner (oder einem anderen Rechner mit angeschlossenem Video-Projektor) gestarteten E-Mail-Server. Eingangs 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/ der Lehrer die Kommunikation stört.

Simuliert werden in diesem Zusammenhang:

- das Vortäuschen einer falschen Identität auf Client-Seite
- das Mitlesen von Nachrichten inkl. Zugangsdaten zum Postfach auf dem Kommunikationsweg
- die Manipulationen von Nachrichten auf dem E-Mail-Server

Das Mitlesen der Zugangsdaten ist mit *Socket Sniff* nicht möglich. Hier bietet sich das wesentlich mächtigere Netzwerkanalysewerkzeug *Wireshark* an (Nutzung nur durch den/die Lehrer/in, siehe Anleitung "Netzwerkcommunication mit *Wireshark* analysieren").

Der Lernabschnitt soll die Schülerinnen und Schüler für die Gefahren bei der Nutzung von E-Mail-Systemen sensibilisieren. Dabei bereitet er die Grundlage, die Verschlüsselung von Kommunikation als Notwendigkeit anzusehen. Das Argument „Ich habe nichts zu verbergen – warum sollte ich also meine Kommunikation sichern?“ wird in den Unterrichtsstunden unter anderem dadurch entkräftet, dass aufgezeigt wird, dass nicht nur das Mitlesen von E-Mails, sondern auch deren Manipulation mit einfachen Mitteln zu bewerkstelligen ist. Ziel ist es, dass die Schülerinnen und Schüler erkennen, dass elektronische Kommunikation die gleichen Anforderungen erfüllen sollte wie die Kommunikation per Post: Vertraulichkeit, Integrität und Authentizität. Wie diese drei Kernanforderungen durchgesetzt werden können und welche Aufgaben und Probleme sie der Informatik stellen, ist das Thema der folgenden Stunden – der Lernabschnitt wirft somit eine grundlegende Fragestellung der gesamten Unterrichtseinheit auf.

Sachanalyse

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. Die Angriffe können dabei sowohl zielgerichtet gegen Personen oder Institutionen (bzw. „User“), als auch breit gefächert gegen unbestimmte Ziele stattfinden.

Die Angriffsmethoden sind dabei vielfältig – in dem vorliegenden Unterrichtsabschnitt werden exemplarisch drei Methoden analysiert. Grundsätzlich kann man zwischen zwei Formen von Angriffen unterscheiden: den „harten“, die ausschließlich durch technische Methoden realisiert werden und die „weichen“, die auf der Erlangung von relevanten Informationen durch sozialen Kontakt zum Angriffsziel basieren (Stichwort: „social hacking“). Die drei Gefahren, die Inhalt des Lernabschnitts sind wurden so gewählt, dass die Schülerinnen und Schüler in der Lage sind, die drei Anforderungen an sichere Kommunikation (Integrität, Authentizität und Vertraulichkeit) zu erarbeiten:

Das Vortäuschen einer falschen Identität auf 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. Eine solche Manipulation kann ohne großen Aufwand mittels Programmen wie *Outlook* oder *Thunderbird* durchgeführt werden (Informationen zu Durchführung siehe unten: „Informationen zur Durchführung“). Für diese Art der Manipulation ist kein Zugriff auf ein fremdes E-Mail-Konto von Nöten.

Das Mitlesen von E-Mails (inklusive übermittelter Passwörter) kann über einen so genannten „man-in-the-middle-attack“ durchgeführt werden. Der Angreifer benötigt dafür Zugriff auf einen Vermittlungsrechner (den er selbst künstlich zwischenschaltet). Er kann somit jeglichen Datenverkehr eines Netzes über den „gefälschten“ Vermittlungsrechner leiten und diesen mittels spezieller Programme (z.B. *Wireshark*) mitlesen. Filtert man diesen Datenverkehr nach den einschlägigen Protokollen (POP3, SMTP), so können gezielt E-Mail-Verbindungen analysiert werden. Die dadurch gewonnen Passwörter können anschließend dafür genutzt werden, sich in das angegriffene Mailkonto einzuloggen.

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

Es sei an dieser Stelle noch einmal darauf hingewiesen, dass der Lernabschnitt nur einen Ausschnitt der möglichen Angriffsmethoden behandelt. An dieser Stelle können natürlich nach Belieben auch weitere Methoden behandelt werden (z.B. Angriffe über die „Sicherheitsfrage“ von E-Mail-Konten oder „social hacking“).

Standardbezug

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.

Stunde 4/5: Gefahren bei der Kommunikation über öffentliche Netzwerke entdecken

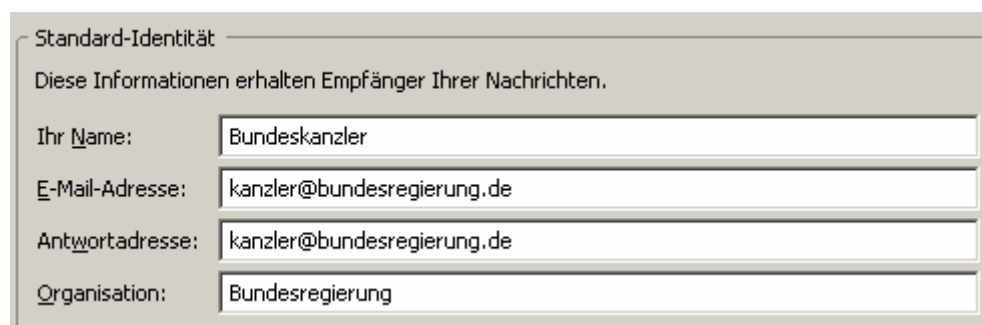
In diesem Lernschritt werden die Schülerinnen und Schüler in einer fiktiven Situation verschiedene reale Gefahren der Kommunikation im Internet erleben. Dazu senden sie sich – wie bereits im Lernschritt zur Rekonstruktion der Protokolle SMTP und POP3 – fiktive Nachrichten über einen auf dem Lehrerrechner (oder einem anderen Rechner mit angeschlossenem Video-Projektor) laufenden E-Mail-Server.

Um einen „man-in-the-middle“-Spionageangriffs auf dem Kommunikationsweg realistisch demonstrieren zu können wird empfohlen, einen Standardrechner als Vermittlungsrechner (Router) umzubauen (Die separate Anleitung "Einen Windows-Rechner zum Router machen" erklärt dies für das Betriebssystem Windows.). 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 Dienstbringer dann nicht mehr deutlich erkennbar. In jedem Fall reichen die Mittel von *Socket Sniff* nicht aus, um Passwörter, die Schülerinnen und Schüler für die fiktiven E-Mail-Konten nutzen, auszuspähen, da der E-Mail-Server Hamster diese ausblendet und eine Aufzeichnung der Kommunikation des Hamsters mit *Socket Sniff* nicht möglich scheint. Es wird daher empfohlen, dass Lehrende auf die Verwendung von *Wireshark* zurückgreifen.

Vorbereitung

Vor dem Unterricht sollten Lehrende ggf. den Router vorbereiten (siehe separate Anleitung) und das spätere Versenden einer E-Mail mit gefälschten Absender-Angaben wie folgt vorbereiten:

- a) Einen weiteren Schülerrechner starten und sich an dem Rechner anmelden.
- b) Einen E-Mail-Client (z. B. *Thunderbird*) starten und für einen gültigen Benutzer des E-Mail-Servers einrichten (siehe Anleitung „E-Mail-Client *Thunderbird* einrichten“).
- c) Die Einstellungen zur Identität abändern:
 - Menü „Extras > Konten“ wählen.
 - Die Angaben zur Standardidentität ändern, z. B.:



Standard-Identität

Diese Informationen erhalten Empfänger Ihrer Nachrichten.

Ihr Name:	Bundeskanzler
E-Mail-Adresse:	kanzler@bundesregierung.de
Antwortadresse:	kanzler@bundesregierung.de
Organisation:	Bundesregierung

- d) Eine E-Mail mit einer vermeintlich vertrauensvollen Information (z. B. Ankündigung einer bevorstehenden Privatisierung eines Staatsunternehmens mit Empfehlung eines Aktienkaufs vor Veröffentlichung des Vorhabens) an den Kurs schreiben und speichern (NOCH NICHT SENDEN – die Postfächer werden ja erst noch erstellt!). Dabei können als Email-Adressen jeweils <vornameDesSchuelers>@<RechnernameDesServers> angenommen werden.

Durchführung

Das folgende Szenario lässt sich in ca. 45 Minuten durchspielen. Für eine Sicherung der Sicherheitsanforderungen an Kommunikation Vertraulichkeit, Integrität und Authentizität ist zusätzliche Zeit zu veranschlagen.

1. Benutzer für die Kursteilnehmer neu einrichten, dabei sollten die Schüler ihre Passwörter selbst eingeben (z. B. durch Herumreichen der Tastatur) – die Schülerinnen und Schüler sollten zuvor darauf hingewiesen werden, nicht Passwörter zu wählen, die sie auch für andere Zugänge nutzen. Warum? Die Passwörter werden ja später in den POP3-Nachrichten ausgelesen – das wiederum den Schülerinnen und Schüler noch nicht sagen!

Vortäuschen einer falschen Identität auf Client-Seite

2. Die Schülerinnen und Schüler auffordern, die Einstellungen ihrer E-Mail-Clients ggf. anzupassen und sich einige E-Mails zu schicken.
 - a) Dabei die unter falscher Identität erstellte E-Mail an den Kurs versenden.
 - b) Anschließend mit *Wireshark* auf dem „Router“ das Passwort eines Schülers „abfangen“.
3. Schülerinnen und Schüler im Plenum versammeln und nach erhaltenen E-Mails befragen („Hat alles geklappt?“, „Irgendwelche Probleme oder Unregelmäßigkeiten?“).
 - a) Die offensichtlich unautorisierte E-Mail wird zum Anlass genommen, festzustellen: „Hier passieren Dinge, die so nicht passieren sollten!“
 - b) Vorschau: „Ich werde jetzt verschiedene Dinge machen.“
 - c) Beobachtungsauftrag: „Notiert:
Welche Gefahren bei der Kommunikation über das Internet lassen sich beobachten?“
4. [Bildschirmprojektion des vorbereiteten Schülerrechners]
Die Einstellungen zur falschen Identität zeigen (siehe Vorbereitung Punkt 3.c).
 - a) „Wie lässt sich feststellen, dass es sich um eine falsche Identität handelt?“
[unglaublich, unpersönlich: der Verfasser weiß nichts über mich.]
„Ja, besser wäre, ich wüsste mehr über die Benutzer der Postfächer ...“

Mitlesen vertraulicher Informationen auf dem Kommunikationsweg

- b) Ein weiteres Konto mit den Benutzerdaten des Schülers, dessen Passwort Sie unter Punkt 2.b ermittelt haben, einrichten, E-Mails anzeigen lassen und eine sehr „unhöfliche“ Antwort verfassen.
„Welche Folgen könnte mein Handeln haben?“
[Streit, der Empfänger nimmt die Nachricht ernst]
„Wie könnte ich auf das Passwort gekommen sein?“
[Verbindung abgehört ...]
- c) [Bildschirmprojektion des „Routers“]
Das Passwort im Protokoll von *Wireshark* zeigen.

Manipulation auf dem E-Mail-Server

5. [Bildschirmprojektion des „Servers“]
 - a) Einen Schüler auffordern, sich mit einem anderen per Email zu verabreden.

- b) Die entstandene .msg-Datei im Ordner Mails\<benutzername> in einem Texteditor öffnen und Zeit und Ort der Verabredung ändern.
- c) Den Empfänger auffordern bitten, sein Postfach auf neue E-Mails zu prüfen.
 "Was machst Du zum verabredeten Termin?"
 [Ich stehe am falschen Ort.]
 "Welche Folgen könnte mein Handeln haben?"
 [Streit, der Empfänger glaubt nicht an eine Manipulation]
 "Wenn sich alle Mitarbeiter des E-Mail-Servers korrekt verhalten – ist dann eine Manipulation ausgeschlossen?"
 [Der Server kann von Fremden gehackt werden.]

Ergebnissicherung

- 6. Abschließend sollten die konkreten Beobachtungen verallgemeinert werden.
 - a) „Was konntet Ihr beobachten?“ Dabei an der Tafel sammeln:
 - Nachrichten mitlesen
 - Nachrichten verändern
 - Nachrichten unter falscher Identität verfassen
 - b) „Was sollte man also sicherstellen?“ Dabei an der Tafel ergänzen:
 - **Keiner kann** Nachrichten mitlesen.
 - **Keiner kann** Nachrichten verändern.
 - **Keiner kann** Nachrichten unter falscher Identität verfassen.
 - c) „Dafür hat man auch Begriffe gefunden.“ An der Tafel ergänzen:

Anforderungen an eine sichere Kommunikation:

 - **Vertraulichkeit:** Keiner kann Nachrichten mitlesen.
 - **Integrität:** Keiner kann Nachrichten verändern.
 - **Authentizität:** Keiner kann Nachrichten unter falscher Identität verfassen.

Vorschau

- 7. „Wir werden zunächst untersuchen, wie sich Vertraulichkeit herstellen lässt! Dieses Problem gibt es nicht erst, seitdem es Computer gibt, die Geheimhaltung von Nachrichten war schon vor tausenden Jahren ein brisantes Thema.“

Material:

- oben stehende Hinweise zur Durchführung als separates Dokument für die Hand des Lehrers
- Anleitung „Einen Windows-Rechner zum Router machen“ für die Hand des Lehrers
- Anleitung „Netzwerk-Kommunikation mit Wireshark analysieren“ für die Hand des Lehrers

Software:

- Wireshark - Netzwerkanalyse-Werkzeug: <http://www.wireshark.org>
 Hinweis: Wird bei der Installation PCap als Dienst installiert (Option im Installations-Dialog aktivieren!), so lässt sich Wireshark auch ohne Administrator-Rechte nutzen.

Lernabschnitt 3: Wie kann ich mit Verschlüsseln Vertraulichkeit herstellen? (10 Stunden)

In dem vorangegangenen Lernabschnitt wurde die Leitfrage aufgeworfen, wie bei der E-Mail-Kommunikation Vertraulichkeit hergestellt werden kann. Die Antwort auf diese Frage liegt nahe: Verschlüsselung! Taucht man tiefer in das Gebiet der Kryptographie ein und setzt es mit dem Informatiksystem E-Mail in Verbindung, so stößt man auf weitere Probleme, deren Lösung Aufgabe der Informatik war (und auch zukünftig sein wird).

Die Schülerinnen und Schüler lernen in diesem Abschnitt der Unterrichtseinheit zunächst klassische Verschlüsselungsverfahren kennen. Dabei erkennen sie – indem sie sich selbst als Kryptoanalytiker versuchen – dass selbst das „Knacken“ komplexer Verschlüsselungen mittels Logik, Kombinatorik und Mathematik mit etwas Übung leicht durchzuführen ist. Dabei erzeugt der Wille der Schülerinnen und Schüler, verschlüsselte Inhalte zu entschlüsseln, erfahrungsgemäß eine hohe Motivation.

Die Behandlung der symmetrischen Verschlüsselungsverfahren endet mit der Erkenntnis, dass es ein Verfahren existiert, das erwiesenermaßen nicht zu entschlüsseln ist („One-Time-Pad“, siehe unten). Die kritische Stelle dieser Verschlüsselung liegt jedoch nicht im Verfahren selbst, sondern in der Übermittlung des Schlüssels. Während in der realen Welt an Handgelenke gekettete Koffer als Transportmittel für Schlüssel eine gewisse Sicherheit bieten mögen, so ist dies mit dem Blick auf den Kontext – E-Mail und Internet – natürlich keine Option.

Der Einstieg in die asymmetrischen Verschlüsselungsverfahren, die den Austausch von Schlüsseln auf einem geheimen Kanal erübrigen, findet anhand des Diffie-Hellmann-Verfahrens statt. Für die Erarbeitung des Verfahrens im Unterricht genügen eine Box und zwei Vorhängeschlösser: Die Schülerinnen und Schüler erhalten die Aufgabe, eine Nachricht an ihre Mitschüler zu senden, ohne dass die Box von einer dritten Partei auf dem Transportweg geöffnet werden kann.

Im letzten Teil des Lernabschnitts werden aktuelle asymmetrische Verfahren am wichtigsten Beispiel RSA erarbeitet. Um die Schülerinnen und Schüler für die Angriffsmöglichkeiten, die auch dieses Verfahren bietet, zu sensibilisieren werden die mathematischen Grundlagen des Verfahrens behandelt und Angriffsmöglichkeiten von RSA aufgezeigt (Stichwort: Primzahlfaktorisation). Am Ende des Lernabschnitts ist somit die Leitfrage beantwortet, wie bei der E-Mail-Kommunikation absolute Vertraulichkeit gewährleistet werden kann – es bleiben noch die Fragen nach der Sicherung von Authentizität und Integrität der elektronischen Post, die in dem nachfolgenden Lernabschnitt 4 beantwortet werden.

Sachanalyse

Die Forderung nach Vertraulichkeit einer Nachricht lässt sich erfüllen, wenn die Nachricht so verschlüsselt wird, dass nur der Empfänger der Nachricht diese wieder entschlüsseln kann. Bei den einfachen „klassischen“ Verfahren lassen sich die Substitution bei denen Zeichen des Klartexts durch andere Zeichen ersetzt werden von der Transposition unterscheiden, bei denen die Zeichen des Klartexts lediglich in ihrer Reihenfolge vertauscht werden. Aus Gründen der Reduktion werden in dieser Unterrichtsreihe Transpositionsverfahren nicht besprochen, bei Interesse und zusätzlicher Zeit bieten sich optionale Exkurse zur Skytale und Fleißnerschen Scheibe an.

Einfache Substitutionssverfahren wie das Caesar-Verfahren 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 Geheimtextalphabetes jedoch in beliebiger Reihenfolge arrangiert, so erhöht

sich die Anzahl möglicher Zuordnungen von 25 beim Caesar-Verfahren erheblich:

$$26! = 403.291.461.126.605.635.584.000.000.$$

Nimmt man an, dass ein Computer zur Anwendung eines Schlüssels 0,01 Sekunden benötigt, so würde ein systematisches Ausprobieren sämtlicher Schlüssels 4.032.914.611.266.056.355.840.000 Sekunden dauern. Da ein Jahr $60 \cdot 60 \cdot 24 \cdot 365 = 31536000$ Sekunden hat, würde das systematische Ausprobieren sämtlicher Schlüssel 127.882.883.411.531.467 Jahre dauern. Bedenkt man, dass die Erde ca. 4.600.000.000 Jahre alt ist, erweist sich das Vorgehen als praktisch unmöglich!

Bei Verfügbarkeit längerer Textpassagen lassen sich jedoch auf Grundlage einer Häufigkeitsanalyse Codezeichen entsprechend der in der Zielsprache typischen Häufigkeit Klartextzeichen zuordnen und die Verschlüsselung so knacken. 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. Wenn das Schlüsselwort allerdings zu kurz gewählt wurde, lässt sich auch eine längere, mit dem dem Vigenère-Verfahren verschlüsselte Nachricht knacken, z. B. durch die Analyse von Parallelstellen (Kasiski-Test). Ist die Länge des Schlüssels erst einmal bestimmt, kann der Text in einzelne Teile zerlegt werden, die dann nur noch mit dem selben Schlüsselbuchstaben verschlüsselt sind und daher leicht entschlüsselt werden können.

Sind die Schlüsselwörter jedoch länger als der Klartext, zufällig gewählt und werden nur einmalig verwendet (Prinzip One-Time-Pad), so garantiert das Verfahren 100%ige Sicherheit. Aufbewahrung und Transport der geheimen Schlüsselwörter, die Absender und Empfänger gleichermaßen benötigen, 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.

Standardbezug

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.

Weiterführende Literatur zum Lernabschnitt 3 „Mit Verschlüsseln Vertraulichkeit herstellen“

- Witten, H.; Letzner, I.; Schulz, R.-H.: RSA&Co. in der Schule, Teil 2: Von Caesar über Vigenère zu Friedman. LOG IN 18 (1998), Heft 5, S. 31-39.
Online verfügbar unter http://bscw.schule.de/pub/bscw.cgi/d637152/RSA_u_Co_T2.pdf
- Witten, H.; Letzner, I.; Schulz, R.-H.: RSA&Co. in der Schule, Teil 3: Flusschiffren, perfekte Sicherheit und Zufall per Computer. LOG IN 19 (1999), Heft 2, S. 50-57.
Online verfügbar unter http://bscw.schule.de/pub/bscw.cgi/d637156/RSA_u_Co_T3.pdf

Optionaler Einstieg: Der Goldkäfer

(eine zusätzliche Doppelstunde zwischen Stunden 4/5 und 6/7)

Eine sehr anschauliche und zugleich spannend beschriebene Anwendung eines Substitutionsverfahrens sowie der Kryptoanalyse durch Häufigkeitsanalyse findet sich in der Geschichte *Der Goldkäfer* [<http://gutenberg.spiegel.de/poe/kaefer1/kaefer1.xml>] von *Edgar Allan Poe* (engl. Original *The Gold-Bug* [<http://www.eapoe.org/works/tales/goldbga2.htm>]). Dieser Abschnitt der Unterrichtseinheit stellt einen optionalen Einstieg in das Thema Verschlüsselung dar und benötigt erfahrungsgemäß eine Doppelstunde. Die im „Goldkäfer“ durchgeführte Dechiffrierung durch den Helden der Geschichte basiert auf einem für die Kryptoanalyse wichtigen Verfahren: der Häufigkeitsanalyse. Ausgehend von der Analyse erschließt sich der Geheimtext durch die Anwendung von Heuristiken, die auf dem Aufbau von Sprache basieren. Die Schülerinnen und Schüler erhalten dabei zunächst nur einen Teil des Textes, der den Lösungsweg zur Dechiffrierung zunächst ausblendet. Aufgabe ist es, nachdem die Häufigkeitsanalyse durchgeführt wurde, selbst Heuristiken zu entdecken, die der Entschlüsselung des Geheimtextes dienen.

Das Auszählen der Häufigkeit der Codezeichen sollte zur Beschleunigung des Verfahrens arbeitsteilig durchgeführt und die Ergebnisse in einer Folie gesammelt werden. Alternativ zum manuellen Auszählen lässt sich die Häufigkeit von Zeichen eines Codes auch gut mit dem Werkzeug *CrypTool* ermitteln:

- Chiffre als Textdatei öffnen oder direkt in das Klartext-Textfeld eingeben,
- dann den Menüpunkt *Analyse > Werkzeuge zur Analyse > Histogramm* wählen.

Auf Grundlage eines Vergleichs des Ergebnis mit der durchschnittlichen Buchstabenhäufigkeit im Deutschen können dann Vermutungen entwickelt werden, die über ein zeichenweises Ersetzen der Zeichen überprüft werden können:

- Menüpunkt *Analyse > Symmetrische Verschlüsselung (klassisch) > Manuelle Analyse > Substitution* wählen

Falls der „Goldkäfer“ nicht als Einstieg in den Lernabschnitt gewählt, sondern nur das Caesar-Verfahren behandelt wird, so sollte in der Caesar-Stunde die Häufigkeitsanalyse als Lösungsmöglichkeit für verschlüsselte Texte behandelt werden. Grund dafür ist, dass das Knacken beliebiger monoalphabetischer Substitutionscodes durch die Häufigkeitsanalyse die Motivation für die Entwicklung von polyalphabetischen Verschlüsselungen darstellte. Möchte man diese wiederum knacken, so muss man sie zunächst auf eine monoalphabetische Verschlüsselung reduzieren, um sie durch eine Häufigkeitsanalyse angreifbar zu machen. Ist für die Unterrichtseinheit genug Zeit vorhanden, empfehlen wir den „Goldkäfer“ als Einstieg in die Verschlüsselung zu wählen – nicht zuletzt weil die Geschichte über Piraten und vergrabene Schätze bei den Schülerinnen und Schülern Spannung, Neugier und somit auch Motivation erzeugt.

Material

- AB „Der Goldkäfer“
- Folie zur Dokumentation der Häufigkeitsanalyse
- Informationen zur Häufigkeit verschiedener Zeichen(-kombinationen)
- Fortsetzung der Geschichte (als HTML-Seiten mit Links zum *schrittweisen Nachvollziehen der Lösung* oder als PDF-Dokument zum ausdrucken und kopieren - Achtung: Text ohne Tabellen!)

Software

- CrypTool (optional) <http://www.cryptool.de/index.php/de.html>

Stunden 6/7: Monoalphabetische Kryptographie – Caesars Geheimcode

Die Schülerinnen und Schüler werden aufgefordert, sich gegenseitig mit Hilfe von je zwei untereinander angeordnet und seitlich gegeneinander verschoben Doppelalphabet-Streifen 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 auch 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 lässt. Falls für den Einstieg in die Verschlüsselung nicht die optionale Doppelstunde „Der Goldkäfer“ gewählt wird, so muss an dieser Stelle auch die Häufigkeitsanalyse als Methode zum Entschlüsseln monoalphabetischer Verschlüsselungen eingeführt werden (siehe oben).

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

Optional kann das Caesar-Verfahren anschließend auch als Programm umgesetzt werden. Der Vorteil daran ist, dass anhand der Thematik „Verschlüsselung“ Programmierkonzepte eingeführt werden können. Es besteht dabei jedoch auch die Gefahr, dass der rote Faden der Unterrichtseinheit verloren geht, da erfahrungsgemäß die Programmierung neue Probleme und Fragen aufwirft, die mit den zentralen Fragestellungen der Unterrichtseinheit keine Verbindung besitzen. Wenn die klassische Kryptographie mit Übungen zur Programmierung verbunden werden soll, erscheint es uns daher sinnvoller, dies in einer vorausgehenden Unterrichtsreihe umzusetzen.

Material

- Arbeitsbogen „Das Geheimnis des römischen Kaisers Caesar“, (Lösung zu Aufgaben 2 und 3)
- 30 Doppel-Alphabet-Streifen
- mit Caesar verschlüsselte Sprüche
- ggf. Codebeispiele

Software

- Krypto 1.5 <http://www.kuehnsoft.de/krypto.php>

Stunde 8: Polyalphabetische Kryptographie – Vigenère und One-Time-Pads

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.

Das Werkzeug *Krypto 1.5* bietet eine sehr anschauliche Animation des Vigenère-Verfahrens. Als Arbeitsauftrag sollten die Schülerinnen und Schüler aufgefordert werden, eine Nachricht, die sie per E-Mail verschicken wollen, mit *Krypto 1.5* unter dem Menüpunkt *Demos >> Vigenère-Verschlüsselung* zu verschlüsseln und dabei die Animation zu beobachten um das Vorgehen zu erklären. Die verschlüsselte Nachricht kann einfach aus dem Chiffre-Feld von Krypto 1.5 in den E-Mail-Client kopiert bzw. aus dem

E-Mail-Client zum entschlüsseln in das Chiffre-Feld von *Krypto 1.5* kopiert werden. Der Arbeitsbogen *Häufigkeitsanalyse mit Vigenere verhindern* bietet geeignete Arbeitsaufträge, durch die die Schülerinnen und Schüler sich die Funktionsweise des Verfahrens anhand der Animation erschließen.

Das Verfahren wurde lange Zeit als sicher angesehen. Wird das Schlüsselwort bei der Verschlüsselung längerer Textpassagen jedoch oft genug angewendet, so treten in der Chiffre aufgrund der in einer Sprache typischen Buchstabengruppen (Bi- und Trigramme) oder auch häufig auftretender kurzer Wörter wie z. B. Artikel wiederkehrende Zeichenkombinationen auf, auf deren Grundlage auf die Länge des Schlüsselwortes geschlossen werden kann. Ist die erst einmal gelungen, so lässt sich auf der Menge der Zeichen, die mit der gleichen Position des Schlüsselwortes verschlüsselt wurden jeweils eine Häufigkeitsanalyse durchführen.

Mit dem Werkzeug *CrypTool* lässt sich zeigen, dass auch diese Verschlüsselung geknackt werden kann (Menü *Analyse >> Symmetrische Verschlüsselung (klassisch) >> Chyphertext Only >> Vigenère*). So könnte z.B. die Lehrkraft eine mit Vigenere 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 (Die gesuchte Person ist Blaise de Vigenere - das müssen die Schülerinnen und Schüler dann wiederum selbst herausfinden).

Aus dieser statistischen Angriffsmöglichkeit folgt die Schlussfolgerung, dass sie bei einer sicheren Verschlüsselung mit dem Vigenère-Verfahren das Schlüsselwort sich – bezogen auf den Klartext - nicht wiederholen darf, d.h. seine Länge sollte größer als die der verschlüsselten Nachricht sein. Außerdem sollte das Schlüsselwort selbst nicht ein natürlichsprachliches Wort sondern eine zufällig erzeugte Zeichenfolge sein, die jeweils nur ein einziges Mal eingesetzt werden darf. Dieses Prinzip (*One-Time-Pad*) wurde z.B. von Agenten im Kalten Krieg eingesetzt (Ein interessanter Bericht zu von Funkern entdeckten merkwürdigen Zahlencodes: <http://www.astrosol.ch/numberstations/>). Das One-Time-Pad verhindert 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.

Material

- Arbeitsbogen „Häufigkeitsanalyse mit Vigenere verhindern“
- Verschlüsselte E-Mail der Polizei, Vorschlag für den Header der E-Mail, (Klartext der Nachricht)

Software

- Krypto 1.5 <http://www.kuehnsoft.de/krypto.php>
- CrypTool <http://www.cryptool.de/index.php/de.html>

Optionaler Exkurs: Vigenère per Hand knacken **(eine zusätzliche Stunde zwischen Stunden 8 und 9)**

Das Knacken einer Vigenère-Verschlüsselung per Hand ist – selbst mit einem arbeitsteiligen Vorgehen – nicht ohne einen gewissen Zeitaufwand durchzuführen. Deshalb schlagen wir vor, diese Stunde nur durchzuführen, wenn die Lerngruppe in der vorangegangenen Stunde Probleme mit dem Verständnis der polyalphabetischen Verschlüsselung hatte.

Im Rückblick auf die letzte Stunde sollte nun überlegt werden, wie ein Knacken der Chiffre möglich

ist. Mit den Arbeitsbögen *Vigenère knacken* kann das Verfahren zur Bestimmung der Schlüsselwortlänge durch den Vergleich der Abstände zwischen Parallelstellen händisch nachvollzogen werden. Je nach Vorkenntnissen der Lernenden sollte die Bestimmung des größten gemeinsamen Teilers ggf. im geführten Unterrichtsgespräch erfolgen. Die Schülerinnen und Schüler sollten nun in die Überlegungen eingebunden werden, wie sich bei bekannter Länge des Schlüsselworts die einzelnen Buchstaben des angewendeten Geheimworts durch eine Häufigkeitsanalyse auf den wiederkehrend durch einen Buchstaben des Geheimworts verschlüsselten Geheimzeichen rekonstruiert werden können. Die Anwendung der Häufigkeitsanalyse für die mit dem 2. bis 7. Buchstaben des Schlüsselworts verschlüsselten Geheimtext sollte dann arbeitsteilig für die jeweiligen Buchstaben des Geheimworts erfolgen - lassen Sie die Schüler einfach von 2 bis 7 reihum abzählen!.

Durch die Bestimmung der Länge des Schlüssels kann die Vigenère-Verschlüsselung auf eine monoalphabetische Verschlüsselung reduziert werden, die wiederum mit dem den Schülerinnen und Schülern bekannten Verfahren der Häufigkeitsanalyse geknackt werden kann. Der Geheimtext wurde so angelegt, dass der am häufigsten auftretende Buchstabe stets dem „E“ entspricht. Das Schlüsselwort für den Text lautet: „LOGISCH“. Anschließend wird das Vorgehen im Plenum schriftlich festgehalten.

Material:

- Arbeitsbögen „Vigenère knacken“, Geheimtext, (entschlüsselter Klartext)

Optional Exkurs: Film „Krieg der Buchstaben“ (eine zusätzliche Doppelstunde zwischen Stunden 8 und 9)

Der BBC-Dokumentarfilm „Krieg der Buchstaben“ (dt., ca. 45 Min.) bietet die Möglichkeit den Kontext „E-Mail“ zu verlassen und das Thema Verschlüsselung aus der Perspektive der historischen Ereignisse des 20. Jahrhunderts zu betrachten. Bevor die Verschlüsselung durch das Aufkommen moderner Kommunikationsmittel in das Blickfeld von Unternehmen und Privatpersonen rückte, war sie im 20. Jahrhundert besonders Mittel von Staat und Militär die eigene Kommunikation geheim zu halten. Der Film bietet den Schülerinnen und Schülern die Möglichkeit, die Funktionsweise historischer Chiffriermaschinen kennen zu lernen (etwa der deutschen Enigma) und mit den im vorangegangenen Unterricht behandelten Verschlüsselungsverfahren in Beziehung zu setzen. Gleichzeitig kann der Film als Anregung für eine Diskussion über Vertrauen bzw. Misstrauen in zwischenstaatlichen Beziehungen dienen, um den Einsatz von Entschlüsselungsmethoden kritisch zu hinterfragen.

Zu diesem Zweck erhalten die Schülerinnen und Schüler Beobachtungsaufträge, die sowohl die technische, als auch die gesellschaftliche Dimension von den im Film vorgestellten Verschlüsselungstechniken betreffen. Nach der Sichtung des Films haben die Schülerinnen und Schüler Zeit, sich über ihre Arbeitsergebnisse auszutauschen, um anschließend im Plenum ihre Ergebnisse und Meinungen zu präsentieren. Erfahrungsgemäß ist die Diskussion über Verschlüsselung sehr fruchtbar, sodass für den Film eine Doppelstunde eingeplant werden sollte.

Material:

- Arbeitsauftrag: Film - „Krieg der Buchstaben“

Stunde 9: 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. Ein klassisches Beispiel dafür ist ein Telefonbuch: Während die Telefonnummer leicht zu finden ist, wenn man den Namen kennt, ist das Auffinden des Namens sehr schwer, wenn nur die Telefonnummer bekannt ist. Auch das Zerreißen ein Blatts Papier lässt sich leicht durchführen, das Zusammenfügen der zerrissenen Teile ist dagegen für den Restaurator eine anspruchsvolle Aufgabe.

Bei einer Einwegfunktion mit Falltür (kurz: Falltürfunktion) gibt es sozusagen 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. In dieser Stunde 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.

Zur Einführung in die asymmetrische Kryptographie wird den Schülerinnen und Schülern der Arbeitsauftrag erteilt, ein Geheimnis mittels einer Kiste zu übertragen, wobei jeder Kommunikationspartner über ein Vorhängeschloss mit passendem Schlüssel verfügt. Damit können sie selbstständig erarbeiten, wie durch eine Trennung von Ver- und inverser Entschlüsselungsfunktion das Übermitteln geheimer Schlüssel vermieden werden kann.

Die Schülerinnen und Schüler teilen sich in zwei Gruppen, um ein Rollenspiel durchzuführen. Jede Gruppe erhält ein Vorhängeschloss, eine der Gruppen zusätzlich einen Karton/Truhe. Die Gruppen erhalten die Aufgabe, eine Nachricht in dem Karton an die andere Gruppe zu versenden. Dabei muss der Karton den in der Mitte platzierten Lehrer passieren, ohne dass dieser die Möglichkeit hat, die Nachricht zu lesen.

Die Lösung dieses Problems kann mit verschiedenen Verfahren gelöst werden. Im Diffie-Hellmann-Schlüsseltausch schließt die versendende Gruppe den Karton, in dem die Nachricht liegt, mit ihrem Schloss zu und schickt ihn zur anderen Gruppe. Diese Gruppe befestigt ihr Schloss ebenfalls am Karton und schickt ihn wieder zum ursprünglichen Sender zurück. Dieser entfernt nun sein Schloss und sendet den Karton zurück, der nun geöffnet werden kann. Bei dem Diffie-Hellman-Schlüsseltausch handelt es sich nicht um ein vollwertiges asymmetrisches Verschlüsselungsverfahren. Es ist nicht gegen „man-in-the-middle“-Angriffe geschützt, so kann eine übermittelnde Station die Antworten der Kommunikationspartners imitieren und seinen eigenen Schlüssel anstatt denen der Kommunikationspartner übermitteln um so Kenntnis von der übertragenen Botschaften zu erlangen. Der amerikanische Mathematiker ElGamal entwickelt 1985 aus dem Diffie-Hellman-Verfahren ein vollwertiges asymmetrisches Kryptosystem, das auch noch heute verwendet wird.

Um zu verdeutlichen, dass dieses Verfahren auch Angriffsmöglichkeiten bietet und die Lösung des Schlüsseltauschproblems nicht 100%ige Sicherheit bietet, kann das Szenario erneut durchgeführt werden. Diesmal befestigt der Lehrer/die Lehrerin jedoch ein eigenes Schloss an dem Karton und sendet ihn sofort an die sendende Gruppe zurück. Diese entfernt nun korrekterweise ihr Schloss und versendet den Karton erneut. Der Lehrer/die Lehrerin hat nun die Möglichkeit, die Nachricht zu lesen. Gleichzeitig nimmt der Lehrer/die Lehrerin einen baugleichen Karton, der eine eigene Nachricht enthält und sendet ihn – anstatt des Originals – weiter. Der falsche Karton wird durch die Schülerinnen und Schüler mit einem Schloss versehen und an den Lehrer / die Lehrerin zurück geschickt. Nun entfernt er/sie sein/ihr eigenes Schloss und sendet den Karton sogleich zurück (man-in-the-middle-Angriff).

Die Modellierung Diffie-Hellman-Verfahren auf der Ebene von Kisten und Schlössern trennt nicht

zwischen privatem und öffentlichem Schlüssel und ist daher für die Anbahnung des RSA-Verfahrens ungeeignet. Entdecken die Schülerinnen und Schüler das Diffie-Hellman-Verfahren, so sollte durch die Demonstration des man-in-the-middle Angriffs eine weitergehende Überlegung motiviert werden, wie sich ein Austausch der Schlösser verhindern lässt. Hier sollte der Lehrer/die Lehrerin das Szenario gezielt erweitern und ein Treffen der Kommunikationspartner zur Vorbereitung der späteren Kommunikation vorschlagen, wobei nach wie vor keine geheimen Informationen ausgetauscht werden sollen. Es bietet sich an, dass die Gruppen im Vorfeld der Kommunikation ihre Schlösser austauschen (die dann die öffentlichen Schlüssel symbolisieren) und dabei die zum Aufschließen notwendigen Schlüssel (die privaten Schlüssel im Sinne der asymmetrischen Kryptologie) behalten. Nun kann die Kiste direkt von der sendenden Gruppe mit dem Schloss der empfangenden Gruppe verschlossen und nur von der empfangenden Gruppe wieder geöffnet werden.

Abschließend sollten die Schülerinnen und Schüler aufgefordert werden, das zuletzt beschriebene Verfahren schriftlich festzuhalten und die Trennung von Ver- und Entschlüsselungsfunktion als zentrale Idee der Lösung zu benennen.

Material

- 2 Kisten, an denen sich je 2 Vorhängeschlösser anbringen lassen
- 3 Vorhängeschlösser mit Schlüssel (je für Gruppe 1, Gruppe 2, Lehrer)
- Folie mit Arbeitsauftrag „Asymmetrisch verschlüsseln ohne Austausch geheimer Informationen“ am Beispiel eines Vorhängeschlosses

Optionaler Exkurs: Mathematische Umsetzung des Diffie-Hellman-Verfahrens (eine zusätzliche Stunde zwischen Stunden 9 und 10)

Für mathematisch interessierte Lerngruppen bietet es sich an, die mathematische Umsetzung des Diffie-Hellman-Verfahrens zu erarbeiten. Dazu eignet sich der Arbeitsbogen von Johann Penon (s. u.) sowie eine sehr schöne Veranschaulichung im Programm *CrypTool* unter *Einzelverfahren* → *Protokolle* → *Diffie-Hellman-Verfahren*. Fundierte Informationen zu dem Diffie-Hellman-Verfahren erhält man z. B. in der Online-Hilfe sowie im Skript von *CrypTool*. Zum „Knacken“ dieses Systems werden im Gegensatz zur Primfaktorzerlegung bei RSA der diskrete Logarithmus bestimmt.

Material:

- Arbeitsbogen von Johann Penon zum Diffie-Hellman-Verfahren:
http://oszhandel.de/gymnasium/faecher/informatik/krypto/diffie_hellmann_merkle.html

Weiterführende Internetquellen zu Diffie-Hellman- und ElGamal-Verfahren:

- Reischuk, R.; Hinkelmann, M.: Einweg-Funktionen. Vorsicht Falle – Rückweg nur für Eingeweihte! <http://www-il.informatik.rwth-aachen.de/~algorithmus/algo17.php>
- Wikipedia-Eintrag zum Diffie-Hellman-Verfahren:
<http://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch>
- Wikipedia-Eintrag zum ElGamal-Verfahren:
<http://de.wikipedia.org/wiki/Elgamal-Kryptosystem>

Stunde 10: Das Prinzip der asymmetrischen Kryptologie

Die Schülerinnen und Schüler erarbeiten sich mit der Animation "Vertraulichkeit und Authentizität durch asymmetrische Kryptologie herstellen" das Prinzip der asymmetrischen Kryptographie. Sie knüpfen an das aus der letzten Stunde bekannte Schlüsselaustauschverfahren an und setzen es in den Kontext E-Mail. Dabei lernen sie die Funktion von öffentlichen und privaten Schlüssel kennen. Eine Anleitung zur Bedienung der Animation ist auf der dazugehörigen Webseite vorhanden, es wird jedoch empfohlen, den Schülerinnen und Schülern die Anleitung in Papierform zu Verfügung zu stellen, um ein ständiges auf- und abscrollen zu vermeiden. Nachdem die Schülerinnen und Schüler sich die Funktionsweise der asymmetrischen Kryptographie erarbeitet haben, sollen sie diese in Partnerarbeit in einem zusammenhängenden Text verschriftlichen.

Diese Stunde legt die Grundlage für die Beschäftigung mit RSA, während der eigentliche Verschlüsselungsvorgang hier noch als „Black-Box“ funktioniert.

Sollte die Erarbeitung der Animation auch nach erfolgreicher Sicherung des Verfahrens die Stunde nicht füllen, so kann bereits hier thematisiert werden, dass die Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers wie auch alle zuvor besprochenen Verfahren keine Aussagen über die Authentizität des Absenders und die Integrität der Nachricht zulässt. Während die Integrität der Nachricht nur durch Erstellen und „signieren“ eines Hashwerts sichergestellt werden kann, so kann die Authentizität des Absenders bereits hier belegt werden, wenn dieser eine zuvor vereinbarte Nachricht (z.B. seinen Vornamen) mit seinem *privaten* Schlüssel verschlüsselt. Dieses „vertauschen“ der Schlüssel um einen anderen Zweck zu erfüllen sollte nur dann bereits in dieser Stunde besprochen werden, wenn das Verständnis für die Herstellung von Vertraulichkeit sichergestellt ist, da sonst die Gefahr besteht, beide Prozesse und die Zuordnung der Schlüssel zu vermischen.

Material

- Animation (auch als ZIP-Datei zum elektronischen Verteilen verfügbar, ggf. alternative Version zum Verschlüsseln einzelner Zahlen)
- Arbeitsbogen mit Arbeitsaufträgen zur Animation (Schülerinnen und Schüler müssten sonst ständig zwischen Animation und Aufträgen auf und ab scrollen.)

Stunde 11: Konstruktion einer mathematischen Falltürfunktion – Semiprimzahlen und Zerlegung in Primfaktoren

In den vorangegangenen Stunden haben die Schülerinnen und Schüler bereits ein Beispiel für eine Einwegfunktion mit Falltür (auch Falltürfunktion genannt - vom engl. „trap door function“) kennen gelernt: das Vorhängeschloss. Für die asymmetrische Verschlüsselung ist aber eine andere Falltürfunktion von Interesse – die Primzahlfaktorisation: 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. 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 üblichen Schlüsselgrößen (mind. 1024 Bit) unmöglich, aus diesem Produkt auf die Primfaktoren zu schließen. Die erforderlichen Schlüsselgrößen werden durch den RSA-Faktorisierungswettbewerb ermittelt. Die größte Zahl, die in diesem Wettbewerb bisher faktorisiert wurde, ist die RSA-768, die – wie der Name sagt – 768 Bit groß ist. Weil man annimmt, dass die Zahl RSA-1024 bis zum Jahr 2020 zerlegt sein wird, gelten 1024-Bit-Verschlüsselungen ab 2014 als nicht mehr sicher. Man nimmt an, dass mindestens 2048-Bit-Verschlüsselungen für viele Jahre ausreichende Sicherheit bieten – mit zunehmender Rechenleistung (oder dem Erfinden eines

revolutionären Verfahrens zur Primzahlfaktorisation) 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 (Semi)Primzahlen erläutert und ein Verfahren eingeführt, das das Auffinden von Primzahlen ermöglicht (Sieb des Eratosthenes). Abschließend sollen die Schülerinnen und Schüler 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 ohne Hilfe eines Rechners nicht mehr durchzuführen ist.

Material

- Arbeitsbogen „Primzahlen finden mit dem Sieb des Eratosthenes“,
- Sieb des Eratosthenes,
- Animation des Sieb des Eratosthenes: <http://www.hbmeyer.de/eratosib.htm>

Weiterführende Literatur und Weblinks zu Stunde 11:

- RSA-Faktorisierungs-Wettbewerb:
<http://www.rsa.com/rsalabs/node.asp?id=2092>
http://en.wikipedia.org/wiki/RSA_Factoring_Challenge
- Übersicht aller RSA-Zahlen auf Wikipedia:
http://en.wikipedia.org/wiki/RSA_numbers
- Witten, H.; Schulz, R.-H.: RSA&Co. in der Schule. Neue Folge, Teil 4: Gibt es genügend Primzahlen für RSA? Im Druck.

Stunden 12/13: Implementierung asymmetrischer Kryptologie am Beispiel RSA

Das 1978 entwickelte RSA-Verfahren ist ein asymmetrisches Verschlüsselungsverfahren, das genügend große Semiprimzahlen nutzt, um die nötige Sicherheit des Verfahrens zu gewährleisten (z. Zt. 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“ kennen gelernt.

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 AB zum modularen Rechnen führt die SuS in diese für sie ungewohnte Rechenart ein, ein weiterer AB zum modularen Potenzieren kann bei Bedarf zusätzlich eingesetzt werden. Möglich ist auch ein Exkurs zu dem „Square and Multiply“ Algorithmus, so wie er im Artikel „RSA&Co., Neue Folge Teil 1“ ausführlich beschrieben wird (s. Literatur). Dieser Algorithmus lässt sich auf die sog. äthiopische oder auch russische Bauern-Multiplikation aus der Unterhaltungsmathematik zurückführen.

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 Chiffre 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) ein Chiffre zur Verfügung stellen. Gemeinsam versucht die Lerngruppe, den Modul zu faktorisieren. Sind die beiden Faktoren gefunden, so kann das Produkt $\phi(N) = (p-1) \cdot (q-1)$ berechnet werden. Nun muss nur noch eine Zahl d (der geheime Schlüssel) gefunden werden, für die gilt: $(d \cdot e) \bmod \phi = 1$. Mit dem gefundenen Schlüssel kann nun die Chiffre geknackt werden!

Wenn genügend Zeit vorhanden ist, kann zur Übung und Festigung des Umgangs mit dem RSA-Verfahren auch ein kleiner „Chiffrierwettbewerb“ eingeschaltet werden. Zweierteams von SuS wählen sich einen passenden Namen wie „Blehtley Park“, „Room 40“, „Black Chamber“ usw., überlegen sich ein RSA-Schlüsselsystem und veröffentlichen an der Tafel ihren öffentlichen Schlüssel zusammen mit einer chiffrierten Botschaft. Die Aufgabe für die Teams ist es dann, die von den anderen Teams veröffentlichten Schlüssel und Botschaften zu knacken. Dabei wird auch deutlich, dass man beim RSA-Verfahren genau zwischen dem Modul N für das Ver- und Entschlüsseln und dem Modul $\phi(N)$ für das Erzeugen des Schlüsselpaares unterscheiden muss – jedenfalls ist die Verwechslung dieser Module nach unserer Erfahrung die häufigste Fehlerquelle, wenn das von den SuS erdachte System nicht funktioniert.

Ohne den erweiterten Euklidischen Algorithmus ist es – besonders bei größeren Schlüsseln – sehr aufwändig, die zu einer gegebenen Zahl e inverse Zahl d zu finden. Wenn dieses Problem in die Tiefe gehend behandelt werden soll, bietet sich ein weiterer Exkurs zu diesem Algorithmus an. Eine Unterrichtsskizze hierzu findet sich in „RSA&Co., Neue Folge Teil 2“ (s. Literatur). Für diese Unterrichtsreihe haben wir uns aber entschlossen, die mathematischen Anteile möglichst knapp zu halten, um den roten Faden „Sicherheitsprobleme bei der E-Mail-Kommunikation“ nicht aus den Augen zu verlieren. Deshalb haben wir uns für den Einsatz der RSA-Demo von CrypTool entschieden; hier sind die genannten Algorithmen bereits eingebaut und stehen als „Black Box“ zur Verfügung.

Material:

- optionaler Arbeitsbogen „Modulares Potenzieren“, Lösungsbogen
- Arbeitsbogen zur Erstellung eines RSA-Schlüsselpaares und Regeln zum Ver- und Entschlüsseln, Lösungsbogen
- Arbeitsbögen zum Anwenden des RSA-Verfahrens mit manuellem Verschlüsseln des Geburtstags mit kleinen Schlüsseln

Weiterführende Literatur zu RSA:

- Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule, Neue Folge Teil 1. RSA für Einsteiger. In: LOG IN 140 (2006a), S. 45-54.
Online verfügbar unter http://bscw.schule.de/pub/bscw.cgi/d404406/RSA_u_Co_NF1.pdf
- Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule, Neue Folge Teil 2. RSA für große Zahlen. In: LOG IN 143 (2006b), S. 50-58.
Online verfügbar unter http://bscw.schule.de/pub/bscw.cgi/d404410/RSA_u_Co_NF2.pdf

Stunden 14/15: Sicherheit von RSA

Nachdem die SuS in der letzten Doppelstunde erfahren haben, dass die händische Anwendung des RSA-Verfahrens 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. Zu diesem Zweck soll erneut das Geburtsdatum verschlüsselt werden, diesmal jedoch als große Zahl der Form tmmjjj (z.B. wird der 12.06.1995 zur Zahl 12061995). Auch die Primzahlen sind aus einem Schlüsselsystem mit $n > 32.000.000$ zu wählen. Die Rechnungen werden nun von den Schülerinnen und Schülern mit Hilfe von CrypTool (RSA-Demo) durchgeführt.

Da die Bedienung der RSA-Demo von CrypTool nach unseren Erfahrungen in den Lerngruppen der SekI nicht selbsterklärend ist, erhalten die SuS einen AB, der ihnen die ersten Schritte mit der RSA-Demo erleichtern soll.

Anschließend sollen die o. e. „Geburtsstageszahlen“ mit der RSA-Demo verschlüsselt und vom Kommunikationspartner wieder entschlüsselt werden. Die erste Herausforderung ist dabei, Primzahlen p und q zu finden, deren Produkt (der Schlüssel N) größer als 32.000.000 ist. Als Ansatz hierfür bietet es sich an, die Quadratwurzel aus dieser Zahl zu berechnen (≈ 5700 , nach oben gerundet). Mit der Untergrenze 5700 und der Obergrenze 5800 ist man damit auf der sicheren Seite.

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 öffentlichen Schlüsseln eines Partners Nachrichten zu verschlüsseln. Wenn im oberen Teil des Fensters diesen Knopf (den zweiten von oben) betätigt, verschwindet der eigene geheime Schlüssel und es bleibt nur der eigene öffentliche Schlüssel lesbar. Hat man den vorher nicht notiert, hat man Pech gehabt: Er kommt nicht wieder zurück, wenn man wieder auf den obersten Knopf drückt! Die einfachste Lösung ist es, eine zweite Inkarnation der RSA-Demo zu starten, dann hat man ein Fenster für das eigene Schlüsselpaar und ein zweites für den öffentlichen Schlüssel des Partners.

Nach diesen Vorbereitungen können die gewünschten Daten per mail und copy & paste an den Partner gesendet werden.

Zu Beginn der nächsten Phase stellt der Unterrichtende die folgende Aufgabe: „Alice übermittelt Bob ihr verschlüsseltes Geburtsdatum. Der öffentliche Schlüssel von Bob lautet 65537, der Modul N ist 32442353. Könnt Ihr das Geburtsdatum von Alice auch ohne Bobs geheimen Schlüssel ermitteln?“ Hier sollten die Lernenden zunächst versuchen, diese Aufgabe selbstständig ohne weitere Hilfe zu lösen. Am Lehrertisch liegt ein vorbereiteter AB: „RSA mit CrypTool knacken“, den die SuS holen können, wenn sie gar nicht mehr weiterkommen. Auf diese Weise sollte die Aufgabe von allen relativ schnell zu lösen sein.

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. Bei der RSA-Demo würde man also folgendermaßen vorgehen: Man wählt Primzahlen generieren (Knopf rechts oberhalb der Mitte), gibt bei p und q jeweils 2^{63} als Untergrenze und 2^{64} als Obergrenze an. Damit erhält man 2 verschiedene 64-Bit-Primzahlen, mit dem Knopf „Primzahlen übernehmen“ erhält man den gewünschten 128-Bit-Schlüssel (den Modul N).

Diese Überlegung lässt sich verallgemeinern: Bei einer gewünschten Bitlänge von 2^n wäre 2^{n-1} die Unter- und 2^n die Obergrenze. Wenn man mit diesen Werten experimentiert, zeigt sich, dass 128-Bit-Schlüssel noch sehr leicht mit CrypTool zerlegt werden können.

Material

- Arbeitsbögen zum Anwenden des RSA-Verfahrens mit Computer-gestütztem Verschlüsseln des Geburtsdatums mit größeren Schlüsseln, geeignete Schlüsselpaare
- Anleitung „Ver- und Entschlüsseln mit der CrypTool-RSA-Demo“
- Arbeitsbogen „RSA mit CrypTool knacken“

Software

- CrypTool <http://www.cryptool.de/index.php/de.html>

Lernabschnitt 4: Wie kann ich mit digitaler Unterschrift die Integrität der Nachricht und die Authentizität des Absenders überprüfen? (2 Stunden)

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 2/3 – mittels *Socket Sniff* 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 empfangen.

Sachanalyse

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 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. 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 ein netzartige Struktur, in der jeder Teilnehmer für die Korrektheit einer bestimmten Anzahl von öffentlichen Signaturen bürgen kann.

Standardbezug

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.

Stunde 16: Prinzip der digitalen Unterschrift

In dieser Stunde 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 aus Stunde 11 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.

Material

- Animation (auch als ZIP-Datei zum elektronischen Verteilen verfügbar)
- Arbeitsbogen mit Arbeitsaufträgen zur Animation (Schülerinnen und Schüler müssten sonst ständig zwischen Animation und Aufträgen auf und ab scrollen.)

Stunde 17: Digitale Unterschrift anwenden

Nachdem sich die Schülerinnen und Schüler in den vorangegangenen Stunden die theoretischen Grundlagen der asymmetrischen Verschlüsselung erarbeitet haben, sollen sie sich nun in der praktischen Anwendung dieses Verfahrens üben. Am Ende der Stunde sollen alle Lernenden 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 (resp. *PGP4Win* für *Outlook*) zu erzeugen und zu verwalten, oder alternativ ein (leider zeitlich begrenztes) Zertifikat über ein Trustcenter anzufordern (z.B. bei Trustcenter.de → erzeugen einer sog. „TC Internet-ID“). Mit diesem Schlüsselpaar allein ist das Verschlüsseln von Mails noch nicht zu bewerkstelligen. Zunächst muss den 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 an ihre 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 *Socket-Sniff* 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 dazu in der Lage, ein solches System auf schulfremden PCs zu installieren.

Material

- Anleitung „E-Mails verschlüsseln und digital unterschreiben“

Weiterführende Internetquelle zum Verschlüsseln und Signieren von E-Mails:

- ausführliche Anleitung zum sicheren Versenden von E-Mails mit *Thunderbird/Enigmail* und *OpenPGP* im Cryptoportal: https://www.cryptoportal.org/data/Einsatz%20von%20Sicherer%20Email%20bei%20Schuelern_v1.0.pdf

Software

- *GnuPG* - <http://www.gnupg.org/download/index.de.html#auto-ref-2>
direkter Link zum Windows-Installer:
<ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.10b.exe>
- Addon *Enigmail* für Mozilla *Thunderbird*
<https://addons.mozilla.org/de/thunderbird/addon/71/>
(Dieses Add-On muss ggf. von jedem Benutzer installiert werden. In diesem Fall sollte die *.xpi-Datei in einem Tausch-Verzeichnis bereit gestellt werden.)
- kostenlose "TC Internet-ID"-Zertifikate bei *Trustcenter.de* beantragen:
<https://www.trustcenter.de/cs-bin/MyCert.cgi/de/55>
- *PGP4Win* - PGP-Unterstützung für *MS Outlook* und weitere E-Mail-Client-Software:
<http://www.gpg4win.org>

Lernabschnitt 5: Warum sollte ich sicher kommunizieren? (2h)

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 im Umgang mit dem 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 potentiellen Hacker einen größeren monetären Gewinn verspricht.

In diesem letzten Abschnitt der Unterrichtseinheit sollen die Schülerinnen und Schüler die Einsicht gewinnen, dass sichere E-Mail-Kommunikation nichts mit Paranoia oder 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 China eine nicht-staatlich 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.

Den Nutzen von E-Mail-Sicherheit und den Wert von Kommunikationsfreiheit zu erkennen, sehen wir somit als Bestandteil der Erziehung der Schülerinnen und Schüler zu mündigen Bürgerinnen und Bürgern.

Sachanalyse

Im letzten Lernabschnitt der Unterrichtseinheit wird die Frage „Warum sollte ich sicher kommunizieren?“ exemplarisch durch die Beschäftigung mit vier Themen in einem Gruppenpuzzle (mehr zur Methode Gruppenpuzzle in der Beschreibung der Unterrichtsstunden) beantwortet. Die Themen sind:

1. Das Echelon-System: Das Echelon-System ist ein weltumspannendes Abhörsystem der UKUSA-Staaten (USA, Großbritannien, Australien, Kanada, Neuseeland). Die Existenz des Systems gilt spätestens seit einem durch die EU geführten Indizienbeweis als gesichert („Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation – Abhörsystem ECHELON, 2001/2098 [INI]“). Das System dient hauptsächlich zum Abfangen von Satellitenkommunikation, deren Anteil an der globalen Kommunikation ca. 5% ausmacht. Das Abhören von Kommunikation ist Staaten nicht per se verboten – solange der Zweck des Abhörens der Abwehr von Gefahren und der Bekämpfung von Drogen-, Waffenhandel, oder sonstiger Kriminalität dient. Seitens der EU besteht jedoch die Befürchtung, dass ein solches System auch zur Wirtschaftsspionage genutzt werden könnte.

2. DE-Mail: DE-Mail ist Bestandteil des so genannten Online-Bürgerportals. DE-Mail soll als eine sichere Kommunikationsstruktur zwischen Bürgern, Behörden, Banken, Versicherungen und Privatfirmen dienen. Da eine offizielle Kommunikation mit Behörden bisher nur durch Briefpost möglich ist, die Behörden aber heutzutage fast vollständig mit elektronischen Mitteln arbeiten, entsteht eine Doppelstruktur aus Papier- und elektronischen Unterlagen. DE-Mail soll es erlauben, rechtsverbindlich auch per E-Mail zu kommunizieren. Das System steckt zur Zeit noch in den Kinderschuhen – grundlegende Sicherheitsbedenken wurden zuletzt von den Datenschutzbeauftragten des Bundes und der Länder geäußert (siehe Arbeitsbogen: DE-Mail). Das Motto von DE-Mail „So einfach wie E-Mail, so sicher wie Briefpost – verschlüsselt, authentisch, nachweisbar“ hängt unmittelbar mit den von den Schülerinnen und Schülern erarbeiteten Anforderungen an sichere Kommunikation zusammen.

3. Kommunikationsfreiheit: Das Themengebiet „Kommunikationsfreiheit“ eröffnet die Frage, wie und warum Staaten E-Mail-Verkehr kontrollieren können. Neben den technischen Aspekten des Abhörens gilt es auch zu beantworten, welches Interesse Staaten daran haben können, die Kommunikation ihrer Bürgerinnen und Bürger zu überwachen. Dabei werden die in Deutschland geltenden Rechtsnormen (Art. 5 Abs. 1 GG) mit Rechtsnormen aus anderen Ländern in Verbindung gesetzt.

4. PGP („Pretty Good Privacy“): PGP ist ein hybrides Verschlüsselungssystem, das asymmetrische Verschlüsselungsverfahren, sowie die digitale Unterschrift nutzt. Auch wenn die technischen Aspekte von PGP innerhalb der Unterrichtseinheit im Mittelpunkt stehen, erlaubt die Beschäftigung mit der Geschichte des Systems einen spannenden Einblick in den Umgang von Staaten mit Verschlüsselungssystemen. Der US-Amerikaner Phil Zimmermann, der PGP entwickelte, stieß in der Anfangszeit von PGP auf heftigen Widerstand von Seiten der Regierung. Der Export des Systems wurde verboten – er fiel unter die geltenden Gesetze für den Waffenexport. Zimmermann umging dieses Verbot, indem er den gesamten Quelltext des Systems in Buchform druckte und veröffentlichte. Freiwillige Helfer im Ausland tippten den Code ab und ermöglichten somit die Verbreitung von PGP. Mittlerweile ist auch in den USA der Export von Verschlüsselungssystemen nicht mehr den strengen Gesetzen des Waffenhandels unterworfen. Diese Episode wirft jedoch – wie auch in den drei anderen Themengebieten – die Frage auf, welches Interesse Staaten an der Kommunikation ihrer Bürgerinnen und Bürger haben können (und haben sollten).

Standardbezug

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.

Stunden 18/19: Gruppenpuzzle zur Informationsfreiheit

Der finale Abschnitt der Unterrichtseinheit wird in Form eines Gruppenpuzzles durchgeführt. Die Arbeitsteilung ist notwendig, um den Schülerinnen und Schülern zu ermöglichen, die Fülle der Informationen zu erfassen und erlaubt es ihnen, sich in kooperativer Arbeit zu üben.

Das Gruppenpuzzle läuft dabei wie folgt ab: Die Schülerinnen und Schüler finden sich in den so genannten Stammgruppen zusammen. Jedes Mitglied der Stammgruppe erhält ein Thema (Themen: Echelon, DE-Mail, PGP und Kommunikationsfreiheit). Anschließend bilden alle Schülerinnen und Schüler neue, so genannte Expertengruppen. Die Expertengruppen setzen sich aus den Mitgliedern der Stammgruppen zusammen, die das selbe Thema besitzen. In den Expertengruppen wird zunächst anhand der Arbeitsblätter und eigener Recherche in Einzelarbeit das Thema erfasst und anschließend in Gruppenarbeit ein 3-5-minütiger Vortrag erarbeitet, der in Folge innerhalb der Stammgruppen gehalten wird. Somit ist jede(r) Schüler(in) für den Lernerfolg seiner Stammgruppemitglieder verantwortlich. Während der Vorträge notieren sich die Zuhörer Stichpunkte, die es ihnen ermöglichen, die Leitfragen des Gruppenpuzzles zu beantworten.

Die Sicherung der Arbeitsergebnisse erfolgt im Plenum: Der Lehrer / Die Lehrerin projiziert die Leitfragen des Gruppenpuzzles per Beamer/OH-Projektor. Die Schülerinnen und Schüler beantworten diese auf Basis ihrer Notizen aus den Vorträgen. Dabei sollten sich die Schülerinnen und Schüler, die „Experte“ in dem Thema sind, zunächst zurückhalten und nur eingreifen, wenn ihre Stammgruppenmitglieder nicht dazu in der Lage sind, die Leitfragen zu beantworten.

Hinweis: Die Methode „Gruppenpuzzle“ erzeugt durch die Gruppenwechsel erfahrungsgemäß ein Durcheinander. Die Hauptaufgabe der Lehrerin / des Lehrers ist es, die Gruppen zu koordinieren. Es wird vorgeschlagen, die Gruppenzugehörigkeiten festzuhalten (vor allem wenn das Gruppenpuzzle auf zwei Einzelstunden aufgeteilt wird). Optimal ist, wenn zwei Räume vorhanden sind, auf die sich die Schülerinnen und Schüler aufteilen können. Die in der Stundenübersicht angegebene Dauer der einzelnen Phasen (s.u.) ist nur ein Richtwert – grundsätzlich sollte gewartet werden, bis alle Gruppen bereit sind, ihren Vortrag zu halten. Ein frühzeitiges Unterbrechen der Expertenphase führt zu einer unzureichenden Qualität der Vorträge.

Material

- Gruppenpuzzle Echelon, DE-Mail, PGP und Kommunikationsfreiheit

Credit

Die kontextorientierte Unterrichtsreihe „E-Mail (nur?) für Dich“ wurde im Rahmen der Berliner Arbeitsgruppe des Projekts „Informatik im Kontext“ erarbeitet von:

- Andreas Gramm
- Malte Hornung
- Helmut Witten