Hier geht es darum, wie man sich mit Schülern dem Thema PGP nähern kann. Ein Aspekt beschäftigt sich damit, was der Anwender unternehmen kann, um einigermaßen sicher zu sein, dass eine E-Mail

1. tatsächlich von dem angegebenen Absender stammt,
2. nur vom Empfänger gelesen werden kann oder
3. Auskunft darüber gibt, ob der Inhalt verändert worden ist.

Das Thema erweitert das Impulsbeispiel E-Mail und Sicherheit um ein asynchrones Verschlüsselungsverfahren.

PGP - Pretty Good Privacy

Mögliche Szenarien

Selbstverständlich gibt es zahlreiche Möglichkeiten, sich dem Thema auf unterschiedlichen Ebenen zu nähern. Examplarisch möchten wir uns auf zwei Ideen beschränken und diese ganz grob skizzieren.

1 Asymmetrische Verschlüsselung am Beispiel von RSA als eine mögliche Komponente von PGP

Helmut Witten und Ralph-Hardo Schulz beschreiben in ihrem zweiteiligen Artikel zu RSA&Co sehr anschaulich wie und in welchem Umfang Schüler in den mathematischen Hintergrund von RSA eindringen und wie sie handlungsorientiert die Verfahren erschließen können. Dazu werden verschiedene Arbeitshilfen (Arbeitsblätter, Handlungsanweisungen, Schemata) angeboten. Die Schüler müssen sich dazu mit Verfahren zum Rechnen mit Primzahlen und zum Bestimmung der Reste bei der Division befassen. Das reicht aus, um am Beispiel kleiner Primzahlen Zeichen mit RSA zu verschlüsseln. Hilfsmittel können dabei sehr variieren, vom Stift über Taschenrechner und CAS-System bis zum Einsatz von Computern und einer Programmiersprache.
Denkbar ist hier auch der Einsatz von fertigen Softwarelösungen wie CrypTool.

2 Digitale Unterschriften zur Authentifizierung von Mails

Jürgen Müller beschreibt einen Ansatz, der, ausgehend vom Problem des Phishing, zu Rechtsfragen im Zusammenhang mit Verträgen und elektronischer Post führt. Anschaulich, problem- und handlungsorientiert können Schüler beim Einsatz eines Mailservers erkennen, wie einfach Mails verändert oder unter falschem Absender versandt werden können. Als eine Lösung schlägt Herr Müller ein kostenloses Zertifikat zum elektronischen Unterschreiben vor. Alternativ kann aber auch mit PGP gearbeitet werden. Als Mailserver wird "Hamster" empfohlen, dem schließen wir uns voll an. Der "Hamster" kann ohne Installation genutzt und schnell und einfach konfiguriert werden. Auf den Schülerplätzen kann dann mit Outlook Express gearbeitet werden oder mit einer portablen Version eines Mailclients.

Eindrucksvoll können Schüler erleben, dass nach digitaler Unterschrift jede Änderung der Mail beim Empfänger beanstandet wird.

3 Projektarbeit

Die beiden Szenarien lassen sich im Rahmen von Projekten (hier meine ich keine Projekte im Informatikunterricht) verbinden. Dabei können mehr praktische Erfahrungen auch mit anderen Umgebungen gesammelt und der Einblick in die hinter PGP stehenden Verfahren vertieft werden. Außerdem besteht die Möglichkeit, das Verschlüsseln und digitale Unterschriften mit verschiedenen Mitteln zu behandeln und so auch ein Gefühl für den damit verbundenen Aufwand zu erzeugen.
Dazu ein paar Aspekte, die als Anlass zur Auseinandersetzung mit Verschlüsselungsverfahren dienen könnten. Diese Liste erhebt keinerlei Anspruch auf Vollständigkeit.

- Gesellschaft - Individuum - Mensch (Philosophie)
- Verträge per Mail? (Wirtschaft und Recht)
- Algorithmen in den Verfahren (Mathematik und Informatik)
- Ideen (Substitutionen, symmetrische oder asymmetrische Verfahren, ...)
- Sicherheit der Verfahren, Zuverlässigkeit und Angriffsmöglichkeiten
- Handhabbarkeit und Aufwand
- praktisches Handling, Software

Empfehlen möchte ich noch die Präsentation und Ausarbeitung von Andreas Grupp zum Thema PGP, die URL steht in den Quellen. Beides kann sehr nützlich sein.

Quellen

Bücher

- [1] Kippenhahn, Rudolf: Verschlüsselte Botschaften, Rowohlt Verlag, 2001
- [2] Beutelspacher, Albrecht: Geheimsprachen - Geschichte und Techniken, Verlag C.H.Beck, 2002

Zeitschriften

- [3] Kryptographie, Spektrum der Wissenschaft Dossier, 4/2001
- [4] Artikel: Witten, Helmut u. Schulz Ralph-Hardo, RSA&Co. in der Schule-Moderne Kryptologie, alte Mathematik, raffinierte Protokolle
  * Teil 1: RSA für Einsteiger, LOG In Verlag, Login 140/2006, ff S. 45
  * Teil 2: RSA für große Zahlen, LOG In Verlag, Login 143/2006, ff S. 50

- [5] Artikel: Müller, Jürgen: Elektronisch unterschreiben
  * Teil 1: Gefahren im Internet, LOG In Verlag, Login 140/2006, ff S. 55
  * Teil 2: Gefahren im Internet, LOG In Verlag, Login 141/142/2006, ff S. 64

Online-Quellen, Software und Material

- [6] PGP
  http://www.pgp.com/de/downloads/desktoptrial/desktoptrial2.html
- [7] GnuPG
  http://www.gnupg.de
- [8] GPG4win, Software und Handbücher
  http://www.gpg4win.org/
- [9] Seahorse, Frontend gpg unter Linux
  http://www.gnome.org/projects/seahorse/
- [10] EnigMail, Plugin für Thunderbird
  http://thunderbird.erweiterungen.de/kategorie/programmoberflaeche_und_konfiguration/
- [11] Cryptool 1.4.0.0, zum Kennenlernen, Experimentieren und Präsentieren von und mit Kryptographiesystemen
  http://www.cryptool.de/
- [12] Elektronikschule Tettnang, Präsentation und Artikel
  http://www.elektronikschule.de/~grupp/pgp/index.html
- [13] Projekt des Bundesministeriums für Wirtschaft und Technologie: GnuPP Software und Handbücher
  http://www.gnupp.de/verschluesselung/index.html
- [14] Bundesamt für Sicherheit in der Informationstechnik BSI
  http://www.bsi.de/index.htm
- [15] Hamster-Mailserver (Software und gute Anleitung)
  http://www.arcorhome.de/newshamster/tgl/misc/hamster_de.html
  http://hamster.volker-gringmuth.de/
- [16] Sicherheit (für kids)
  http://www.blinde-kuh.de/
- [17] Medienportal Thüringen
  http://www.schulportal-thueringen.de