

# **Informatik-Doppelstunde: Sichere E-Mail**

Lehrender:	NN
Mentor:	NN
Ort:	NN
Datum:	25.05.2007
Zeit:	7.45 – 9.20 Uhr
Reihenthema:	Anwendungen und Funktionsweise des Internets
Stundenthema:	Sichere E-Mail

## **1 Betroffene Entscheidungen**

### **1.1 Thematischer Zusammenhang**

Die Schülerinnen und Schüler

- S1 kennen Kriterien zur Bewertung der Sicherheit von symmetrischen Verschlüsselungsverfahren.
- S2 können eine vertrauliche Nachricht als E-Mail versenden.
- S3 können mit Hilfe der elektronischen Signatur authentische E-Mails versenden.

### **1.2 Ziele der Doppelstunde**

Die Schülerinnen und Schüler

- L1 können ein Schlüsselpaar zur Verschlüsselung mit OpenPGP erstellen und mit anderen den öffentlichen Schlüssel austauschen.
- L2 können eine E-Mail ver- und entschlüsseln.
- L3 können eine E-Mail signieren.

### **1.3 Hausaufgaben**

## 1.4 Geplanter Unterrichtsverlauf

Zeit	Dauer	Phase	Teilziel	Inhalt	Methode	Medien
------	-------	-------	----------	--------	---------	--------

1. Stunde						
	15'	Erarbeitung		Dechiffrierung von Texten, die mit Caesar-Chiffre bzw. Skytale-Chiffre verschlüsselt wurden (AB10, Aufgaben 3, 4)	EA	AB
	15'	Ergebnissicherung		Besprechung der Aufgaben und Verallgemeinerung: <ul style="list-style-type: none"> <li>- Schlüsselraum mögliche Schwachstelle beim Angriff mit Brute-Force → kleiner Schlüsselraum</li> <li>- statistische Analyse bei vielen Verfahren möglich → Qualität des Verfahrens (ist bei Skytale nicht so einfach)</li> </ul>	SV, UG	OHP
	5'	Zielorientierung		In der vorangegangenen Stunde: E-Mail-Übertragungsweg → Wer hat Zugriff auf die Nachrichten? Betreiber der Mail-Server, ggf. andere Benutzer des gleichen Rechners Verschlüsselung mit Caesar- oder Skytale-Chiffre nicht sicher; außerdem vorab geheimer Schlüsselaustausch notwendig (nicht über E-Mail möglich) → In dieser Stunde geht es um eine Möglichkeit vertrauliche Nachrichten auszutauschen	UG	
	5'	Erarbeitung		Analogie zur asymmetrischen Verschlüsselung (Vorhängeschloss, verschließbare Schachtel mitbringen): <ul style="list-style-type: none"> <li>- öffentlicher Schlüssel → Vorhängeschloss ohne Schlüssel</li> <li>- privater Schlüssel → Schlüssel zu Vorhängeschloss</li> </ul>	UG	

	10'			Demonstration zum Einrichten des E-Mail-Programms und zur Installation von Enigmail 1. E-Mail-Benutzerkonten einrichten, Hinweis auf IP-Adresse des Servers und Domain der E-Mail-Adressen 2. Installation von Enigmail, Hinweis auf Speicherort auf Server 3. Schlüsselpaar erzeugen, Hinweis auf persönliche Passphrase	LV	CP
<b>2. Stunde</b>						
	35'			Versenden von vertraulichen E-Mails: E-Mail-Konto einrichten, E-Mail-Programm einrichten, Enigmail installieren, Schlüsselpaar erzeugen, Schlüssel austauschen, verschlüsselte Nachrichten verschicken <i>Optional (für Schülerinnen und Schüler, die früher fertig sind): Wenn in dieser Phase noch Zeit sein sollte, können sich die Schülerinnen und Schüler eine E-Mail als Quelltext ansehen mit dem Auftrag, zu erklären warum ein Teil verschlüsselt und ein anderer im Klartext erscheint.</i>	EA	CO
	5'	Ergebnissicherung		Besprechung Aufgabe 1 zum Ablauf der Ver- und Entschlüsselung einer vertraulichen Nachricht mit asymmetrischem Verschlüsselungsverfahren	SV / UG	OHP
<i>voraussichtliches Ende der Unterrichtsstunde</i>						
	10'	Ergebnissicherung		<i>Besprechung des Ablaufs zum Versand einer vertraulichen Nachricht mit Demonstration</i>	SV / UG	CP, OHP

**Methoden:**

DE: Demonstrationsexperiment

EA: Einzelarbeit

GA: Gruppenarbeit

LV: Lehrervortrag

SE: Schülerexperiment

SV: Schülervortrag

UG: Unterrichtsgespräch

**Medien:**

AB: Arbeitsblatt

OHP: Overhead-Projektor

CO: Computer

TA: Tafel

CP: Computerprojektion

TB: Tafelbild

FO: Folien

## 2 Begründung zentraler didaktischer Entscheidungen

### 2.1 Lerngruppe

Der Kurs besteht aus 3 Schülerinnen und 21 Schülern. In diesem Schuljahr hat der Informatikkurs begonnen. Bisher wurde objektorientierte Programmierung mit Java und dem Konzept zu „Stiften und Mäusen“ und BlueJ im Unterricht behandelt. Dazu wurden bereits Klassendiagramme mit verschiedenen Beziehungen behandelt. Außerdem wurde eine Unterrichtsreihe zum Thema endliche Automaten durchgeführt. In einer Stunde wurden zudem Kenntnisse zum Binärsystem wiederholt.

### 2.2 Begründung der Inhalte

### 2.3 Begründung des Lernweges

OpenPGP spezifiziert zwei Verfahren für den Sicherheitsdienst Vertraulichkeit: ein symmetrisches Verfahren und ein Public-Key-Verfahren. Beim Public-Key-Verfahren wird für jede Nachricht ein zufälliger Sitzungsschlüssel generiert. Die Nachricht wird mit diesem Schlüssel und einem symmetrischen Algorithmus verschlüsselt. Der Session-Key wird wiederum mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der Nachricht hinzugefügt. Es ist demnach ein hybrides Verfahren. Der Einsatz von Hybridsystemen ist nach Schneier [Schneier, 2006, S. 39] aus zwei Gründen sinnvoll:

1. asymmetrische Verfahren sind zu langsam und
2. asymmetrische Verfahren sind anfällig gegen chosen-plaintext-Angriffe, weil immer derselbe öffentliche Schlüssel verwendet wird (aus bekannten n Klartexten kann der übertragene Text bestimmt werden).

Der erste Grund ist für diesen Kontext von untergeordneter Bedeutung, weil E-Mails in der Regel so kurz sind, dass ein langsamerer Algorithmus nicht weiter stört. Das zweite Argument ist dahingehend nicht so gravierend, dass für einen solchen Angriff bereits ein gewisser Aufwand betrieben werden muss, der durch den Wert der übermittelten Nachricht gerechtfertigt sein müsste.

## 3 Literatur

[Bless et al., 2005] R. Bless, S. Mink, E.-O. Blaß, M. Conrad, H.-J. Hof, K. Kutzner, M. Schöller: Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen. Springer, Heidelberg, 2005.

[RFC2440] Request for Comments „OpenPGP Message Format“. 1998. URL: <http://www.ietf.org/rfc/rfc2440.txt> – geprüft: 29.05.2006

[Schneier, 2001] B. Schneier: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt, Heidelberg, 2001.

[Schneier, 2006] B. Schneier: Angewandte Kryptographie. Pearson Studium, München, 2006.