

Informatik-Einzelstunde: Verschlüsselung

Lehrender:	NN
Mentor:	NN
Ort:	NN
Datum:	23.05.2007
Zeit:	11.25 – 12.10 Uhr
Reihenthema:	Anwendungen und Funktionsweise des Internets
Stundenthema:	Verschlüsselung

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 Einzelstunde

Die Schülerinnen und Schüler

- L1 können die Grundoperatoren Substitution und Transposition erklären.
- L2 können Methoden zur Dechiffrierung bei bekanntem Geheimtext („Brute Force“ und statistische Analyse) anwenden.

1.3 Hausaufgaben

1.4 Geplanter Unterrichtsverlauf

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

1. Stunde						
11.25	15'	Wiederholung		Besprechung der Aufgabenlösung → Problem: Authentifizierung Wichtige Zusammenhänge: - Analogie Postversand - Authentifizierung - SMTP und POP3 - Begriff Protokoll	UG	OHP, TA
11.40	5'	Zielorientierung		„Wie ist es möglich, eine geheime Nachricht im Klassenraum auszutauschen, wenn man nicht sicher ist, dass niemand unbefugtes die Nachricht liest?“ → Verschlüsselung Das Problem ist der unsichere Übertragungskanal. In welchen Fällen tritt das auch sonst auf? → In der Stunde zum E-Mail-Versand wurde deutlich, dass die Nachrichten im Klartext auf jedem Rechner, der an der Übertragung beteiligt ist, vorliegt. Es besteht keine Möglichkeit der Zugriffskontrolle für Absender und Empfänger.	UG	
11.45	20'	Erarbeitung		Expertenpuzzle mit vier Gruppen zu den Verschlüsselungsverfahren Caesar-Chiffre und Skytale-Chiffre (Substitution und Transposition), Expertenpuzzle, (AB, Aufgabe 1,2)	GA	AB

	10'	Ergebnissicherung		optional: Präsentation zu den Verschlüsselungsverfahren und zum Vergleich der Verfahren - am Beispiel die zwei Verfahren erläutern - Vergleichstabelle erklären	SV	TA
	10'	Erarbeitung		Dechiffrierung mit Brute-Force (AB, Aufgabe 3)	EA	AB
	10'			optional: Dechiffrierung mit statistischer Analyse (AB, Aufgabe 4)	EA	AB
				-		

Methoden:

DE: Demonstrationsexperiment

EA: Einzelarbeit

GA: Gruppenarbeit

LV: Lehrervortrag

SE: Schülerexperiment

SV: Schülervortrag

UG: Unterrichtsgespräch

Medien:

AB: Arbeitsblatt

CO: Computer

CP: Computerprojektion

FO: Folien

OHP: Overhead-Projektor

TA: Tafel

TB: Tafelbild

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

Ziel des Themas Verschlüsselung ist es, dass die Lernenden verstehen, was Verschlüsselung ist und diese verantwortungsvoll einsetzen. Dazu ist es notwendig, dass ein Bewusstsein dafür besteht, dass nicht jede Verschlüsselung auch Vertraulichkeit gewährleistet. Es muss deutlich werden, dass zum einen ein zu kleiner Schlüsselraum die Sicherheit gefährdet und zum zweiten mögliche Schwachstellen des Verfahrens andere Angriffsmöglichkeiten bieten. Anhand einfacher Verfahren, die auf den Grundoperationen Substitution und Transposition beruhen, wird zum einen die grundsätzliche Verfahrensweise zur Verschlüsselung deutlich. Zum anderen eignen sich solch einfache Verfahren auch, Dechiffrierung durch Brute-Force und durch statistische Analyse zu verdeutlichen.

2.3 Begründung des Lernweges

3 Literatur

[Kurose/Ross, 2002] Kurose, J. F.; Ross, K. W.: Computernetze. Pearson Studium, München, 2002, S. 557-561.

[Schneier, 2006] Schneier, B.: Angewandte Kryptographie. Pearson Studium, München, 2006, S. 11-15.