ETH Institut für Verhaltenswissenschaft; Departement Informatik

---

Gruppenunterricht zum Thema:
Kryptografie und Kryptoanalyse

Fach:
Informatik, Informationssicherheit

Schultyp:
Sekundarstufe II (Gymnasien, Berufsschulen) letzte Klassen, Technikerschulen, Fachhochschulen

Vorraussetzungen der Adressaten:
Grundkenntnisse der Internetanwendungen (Internet, E-Mail…)
Mathematische Grundkenntnisse

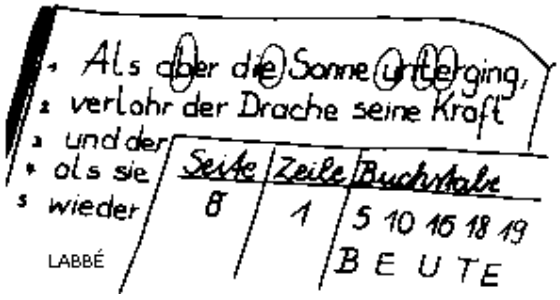
Art der Gruppenarbeit:
Kleingruppenarbeit

Dauer:
2 Lektionen

Autor:
Marcel Kessler

Beiträge:
Michael Näf (Konzept), Ralph Morelli (Framework)

Fassung vom:
1. Oktober 2003



Inhalt

Informationen für die Lehrperson

1. Leitideen

Die wachsende Bedeutung von Internet und E-Mail bringt einen zunehmenden Datenaustausch mit sich. Immer mehr Leute versenden und empfangen Nachrichten. Deshalb muss man sich vermehrt Gedanken über die Sicherheit der Nachrichten machen. Hier setzen Verschlüsselungsverfahren an.
Die modernen Verschlüsselungsverfahren sind meist relativ kompliziert. Sie basieren aber auf denselben Prinzipien wie die einfachen und verständlichen „historischen" Verfahren. Deshalb sollen anhand praktischer Erfahrungen mit diesen „klassischen" Verfahren die Grundlagen der Verschlüsselung kennen gelernt werden.
Auch in der Kryptoanalyse funktionieren zum Teil noch die gleichen „Tricks" wie bei den „historischen" Verfahren. Durch Experimentieren mit verschiedenen - ebenfalls „klassischen" - Analysemethoden soll klar werden, welche Möglichkeiten es gibt eine verschlüsselte Nachricht zu „knacken".

2. Dispositionsziele

- Die Adressaten erkennen, dass Verschlüsselung eine Technik ist um Vertraulichkeit zu gewährleisten. Es sollte ihnen dabei auch bewusst werden welches trotz Verschlüsselungsverfahren die Restrisiken sind.
- Die Adressaten sind sich der Gefahren beim unverschlüsselten Nachrichtenaustausch bewusst, kennen aber auch um die Probleme, die eine Verschlüsselung mit sich bringt.
- Die Adressaten können zu diesem Thema passende Artikel in (Fach-)Zeitschriften in einen Kontext setzen.

3. Operationalisierte Lernziele

- Die Adressaten können anhand historischer Verschlüsselungsverfahren erklären was es braucht um eine Nachricht „sicher" zu übermitteln.
- Die Adressaten kennen die grundsätzlichen Schwachstellen von Verschlüsselungsverfahren, zum Beispiel zu kurze Schlüssellängen.
- Die Adressaten kennen den Unterschied zwischen monoalphabetischen und polyalphabetischen Verschlüsselungsverfahren.
- Die Adressaten können die 3 klassischen Verschlüsselungsverfahren Caesar, Substitution und Vigenère selbst auf eine beliebige Textnachricht anwenden.
- Die Adressaten kennen 2 Methoden der Kryptoanalyse (Brute-Force und Häufigkeitsanalyse) und können diese auf verschlüsselte Texte anwenden.
- Die Adressaten kennen die Begriffe One-Time-Pad, DES und IDEA.

Einbettung in den Gesamtkontext

Diese Unterrichtseinheit versteht sich als eine Einleitung in das Thema der Kryptografie. In einer Gruppenarbeit werden historische Verfahren der Kryptografie und Kryptoanalyse kennen gelernt.
Auf den hier gewonnenen Grundkenntnissen kann dann eine tiefere Behandlung der modernen Verfahren wie DES und IDEA aufsetzen. Die Unterrichtseinheit eignet sich auch als Vorbereitung für asymmetrische Verfahren wie das Public-Key-System.

Anforderung an die Informatik-Infrastruktur

- es braucht pro 2 Studierende einen Java-fähigen PC mit Internetanschluss (siehe dazu auch Datei „READMEFIRST.txt“)
- jeder Studierende benötigt Zugang zu einem E-Mail-Account

Lerntätigkeiten der Schüler/innen oder Studierenden in den vorangegangenen Stunden

Es ist keine spezielle Vorbereitung der Adressaten auf diese 2 Lektionen nötig.

Die einzigen Vorraussetzungen an die Adressaten sind:

- Sie wissen wie man einen Computer bedient und …
- … sie haben Erfahrungen im Umgang mit Internetapplikationen wie E-Mail, Web-Browser etc.

Bemerkungen zum Ablauf des Unterrichts

Der Unterricht beginnt und endet mit einem Lehrervortrag. Dazwischen findet eine Gruppenarbeit statt. Im einleitenden Vortrag sollen die Adressaten bereits die ersten Grundkonzepte und ein erstes Verschlüsselungsverfahren kennen lernen, damit in der Gruppenarbeit nicht mehr Theorie als nötig vorkommt.
In der Gruppenarbeit sollen die Adressaten vor allem praktische Erfahrung mit den Verschlüsselungsverfahren und mit den Analysemethoden bekommen. Deshalb steht in der Anleitung zur Gruppenarbeit nur so viel Theorie wie unbedingt nötig.
Im abschliessenden Lehrervortrag werden dann die wichtigsten Konzepte nochmals erwähnt, und es werden noch einige moderne Verfahren, die nicht praktisch geübt werden können, vorgestellt.

Lerntätigkeit bis zum Beginn der Gruppenarbeit

1. Einführung (10')

Die Lehrperson hält einen kurzen Vortrag als Einführung ins Thema „Kryptografie und Kryptoanalyse". Dabei wird bereits auf die Problematik des Schlüsselaustausches und auf das Caesar-Verfahren eingegangen.

2. Erklären des weiteren Ablaufs (5')

Die Lehrperson bildet möglichst leistungsheterogene Vierergruppen, welche dann wiederum in Zweierteams aufgeteilt werden. Jedem Zweierteam wird darauf ein Computer zugewiesen, und zwar möglichst in räumlicher Nähe zum anderen Zweierteam der Vierergruppe. Die 2 Zweierteams einer Vierergruppe arbeiten zusammen.

Anleitung zur Gruppenaktivität

Allgemein

Die Studierenden folgen in Zweierteams einer Online-Anleitung und lernen dabei 3 Verschlüsselungsverfahren kennen. Zu jedem Verschlüsselungsverfahren lernen sie auch verschiedene Analysemethoden kennen. Für die Ver-/Entschlüsselung sowie zur Analyse stehen den Studierenden Java-Applets zur Verfügung.

Falls ein Zweierteam zu einer gewissen Zeit unbeschäftigt ist, stehen in der Anleitung diverse Links mit detaillierten Informationen zum jeweiligen Abschnitt. Aufgrund der Kurzlebigkeit von Links im Internet müssen diese Links geprüft und gegebenenfalls durch analoge aktuelle Links ersetzt werden.

In der Anleitung verstreut sind kurze Verständnisfragen, welche von den Studierenden diskutiert und beantwortet werden sollten. Nach der Gruppenarbeit geht die Lehrperson im 2. Teil des Vortrages auf diese Fragen ein.

Die Aktivitäten der Studierenden gliedern sich in 6 Teile und sollen den Studierenden zum einen die Wichtigkeit der geheimen Schlüsselübermittlung zeigen, ihnen jedoch auch klar machen das es für beinahe jedes Verschlüsselungsverfahren (auch für die modernen) eine Analysemethode gibt:

1. Ver-/Entschlüsseln mit Caesar (10')

1) Das Caesar-Verfahren haben die Studierenden im Lehrervortrag kennen gelernt.
2) Die beiden Zweierteams treffen sich persönlich für den Schlüsselaustausch (Zahl zwischen 1 und 26).
3) Beide Zweierteams verschlüsseln mit dem Java-Applet „Caesar" eine Nachricht und senden sie an das andere Team.
4) Die empfangene Nachricht wird mit Hilfe des Schlüssels entschlüsselt.

2. Kryptoanalyse des Caesar-Verfahrens (5')

1) Zuerst wechseln die Studierenden den Platz, so dass das andere Mitglied des Zweierteams den Computer bedient.
2) Sie verschlüsseln wiederum eine Nachricht, mit neuem Schlüssel, und senden diese an das Partnerteam, jedoch ohne den Schlüssel zu übermitteln.
3) Mit den Analysemethoden des Java-Applets versuchen sie nun die „gegnerische" Nachricht ohne Kenntnis des Schlüssels zu knacken. Dabei verwenden sie die Brute-Force-Methode.

3. Ver-/Entschlüsseln mit Substitution (5')

1) In der Anleitung wird auf die Schwächen des Caesar-Verfahrens hingewiesen und ein verbessertes Verfahren erklärt: Substitution.
2) Die beiden Zweierteams treffen sich persönlich für den Schlüsselaustausch (Buchstabenkombination).
3) Beide Zweierteams verschlüsseln mit dem Java-Applet „Substitution" eine Nachricht und senden sie an das andere Team.
4) Die empfangene Nachricht wird mit Hilfe des Schlüssels entschlüsselt.

4. Kryptoanalyse des Substitutionsverfahrens (25')

1) Zuerst findet wieder ein Platzwechsel statt, d. h. derselbe Studierende wie zu Beginn sitzt wieder vor dem Computer.
2) Die 2 Teams schicken sich nun gegenseitig eine neue mit der Substitutions-Methode verschlüsselte Nachricht. In diesem Fall sollte die Nachricht mindestens 200 Zeichen lang sein; der Schlüssel wird wiederum nicht mitgeteilt.
3) Zuerst versuchen die Zweierteams nun die Nachricht mit der Brute-Force-Methode zu knacken, was jedoch nicht gelingt.
4) Mit Hilfe der Häufigkeitsverteilung, den statistischen Informationen und ein wenig logischem Denken und Ausprobieren sollte es den Zweierteams dennoch gelingen, den gegnerischen Text zu knacken. Möglicherweise muss die Lehrperson hier ein wenig unterstützen.

5. Ver-/Entschlüsseln mit Vigenère (5')

1) Nachdem auch die Schwächen des Substitutionsverfahrens aufgezeigt wurden, wird den Studierenden in der Anleitung noch das Vigenère-Verfahren erklärt.
2) Mit dem gleichen Schlüssel wie bei dem Substitutionsverfahren wird mit dem Java-Applet „Vigenère" eine Nachricht verschlüsselt und an das andere Team gesendet.
3) Die empfangene Nachricht wird mit Hilfe des Schlüssels entschlüsselt.

6. Kryptoanalyse des Vigenère-Verfahrens (10')

1) Zuerst wechseln die Studierenden zum letzten Mal den Platz.
2) Die Zweierteams erstellen eine neue Nachricht (wiederum mindestens 200 Zeichen lang) und senden sie an das andere Team, ohne den Schlüssel zu verraten.
3) Danach versuchen sie mit Häufigkeitsanalyse und den Methoden der Substitution die Nachricht des anderen Teams zu knacken.
4) Da es sich um eine polyalphabetische Verschlüsselung handelt, kann dies nicht gelingen, was in der Anleitung erklärt wird.
5) Mit Hilfe der im Applet eingebauten Funktion „Automatische Analyse" soll den Studierenden klar werden dass auch eine mit Vigenère verschlüsselte Nachricht geknackt werden kann. Die Anleitung bietet hierfür nur per Links eine Erklärung (für die welche schneller fertig sind), da die Lehrperson im 2. Teil der Präsentation auf die Analyse des Vigenère-Verfahrens eingeht.

Lerntätigkeit nach der Gruppenarbeit bis zum Ende der Lektion

1. Abschluss (15')

In der Gruppenarbeit haben die Studierenden neu die Verschlüsselungsverfahren Substitution und Vigenère sowie die Analysemethoden Brute-Force und Häufigkeitsverteilung kennen gelernt.

In der zusammenfassenden Präsentation werden die Verfahren und Methoden nochmals kurz rekapituliert und es wird auf die in der Anleitung eingebauten Verständnisfragen eingegangen.

Ausserdem geht die Präsentation noch auf das One-Time-Pad-Verfahren und moderne Verfahren wie DES und IDEA ein. Dabei sollen noch einmal die wichtigsten Konzepte wie „minimale Schlüssellänge" und „geheimer Kanal für den Schlüsselaustausch" betont werden.

In einer weiteren Lektion könnten die Themen „Asymmetrische Verschlüsselung" und „Public-Key-Verfahren" behandelt werden.

Referenzen

Zur Erstellung dieser Gruppenarbeit wurden folgende WWW-Quellen benutzt:

- Descriptions of Historical Ciphers (http://starbase.trincoll.edu/~crypto/historical/)
- Symmetrische/ klassische Kryptographie -- Ein interaktiver Überblick (http://www.wiwi.uni-bielefeld.de/StatCompSci/lehre/material_spezifisch/statalg00/caesar/caesar.html)
- Einführung in die Kryptologie (http://www.regenechsen.de/krypto/substitution.htm)
- The Cryptology Matrix! (http://www.math.nmsu.edu/crypto/public_html/)
- Pommerening: Kryptologie (http://www.uni-mainz.de/~pommeren/Kryptologie/)
- GAT – Kryptologie (http://www.blankenburg.de/gat/pages/fach/info/krypto.htm)
- Klassische Kryptografie (http://www.iti.fh-flensburg.de/lang/algorithmen/code/krypto/klassisch.htm)
- Facharbeit zum Thema Kryptologie (http://www.daniel-faber.org/schule/facharbeit/html/)
- CrypTool (http://www.cryptool.de)