



E-Mail (nur?) für Dich

eine kontextorientierte Unterrichtsreihe

SH-HILL-Tagung in Neumünster

13. November 2010

Andreas Gramm

***1. Schulpraktisches Seminar
Charlottenburg-Wilmersdorf, Berlin***

Was ist „Informatik im Kontext“?



eine ***kontextorientierte*** Unterrichtsreihe zur kritischen Würdigung der Revolution des Briefverkehrs im 20. Jahrhundert

- konzeptionell an naturwissenschaftliche Kontext-Projekte angelehnt:
- Schülerinnen und Schüler erleben Wissen und Strategien in Zusammenhängen.
- Schülerinnen und Schüler erleben Wissen als konstruktiv erleben. → Handlungsorientierung



Die drei Säulen von *inik*:



- Orientierung an Kontexten
- Orientierung an Standards
- Methodenvielfalt

Orientierung an Kontexten



Schülerinnen und Schüler ...

erschließen intelligent vernetztes Wissen
in sinnstiftenden vieldimensionalen Kontexten.

erkennen die Bedeutung des Wissens für die
Lebenswelt bzw. spätere Arbeitswelt.

Orientierung an Standards



GI-Bildungsstandards: <http://www.informatikstandards.de>

Methodenvielfalt



Schülerinnen und Schüler
erschließen sich Wissen
eigenständig und kooperativ

Wer ist „Informatik im Kontext“?

inik
informatik im kontext



- offenes bundesweites Projekt
- Entwicklung und Diskussion unter <http://inik.pbworks.com> (Anmeldung erforderlich)

VIEW **EDIT**

☆ **FrontPage**

last edited by Gramm 2 days ago Page history

Zurzeit in der Entwicklung:

- [E-mail \(nur?\) für Dich!](#) (Andreas Gramm, Helmut Witten, Malte Hornung - Bln)
- [Planspiel zum Datenschutz - Online Version 2.0](#) (Frank Oppermann, Alex Dietz - Bln)
Arbeitsergebnisse Königstein 2009: [Wer weiß was über mich im Internet? - Datenschutzspiel 2.0](#) (Frank, Ira, Michael, Michael)
- [Mobil telefonieren](#) (Andreas Gramm, Carsten Schulte, Johann Penon - Bln)
- [Geschichte der Fernkommunikation](#) (Malte Hornung - Bln)
- [Aktoren und Sensoren - das intelligente Haus mit Scratch und Picoboards](#) (Ralf Kreutel, Ralf Punkenburg - Bln)
- [MP3](#) (Clemens Wagner, Mattias Müller - Bln) - in Arbeit ...
- [WP Informatik und Physik mit Themen Graphik, Sound, ... in der Sek 1](#) (Arno Pasternak) - Material kommt nach Durchführung

Bereits veröffentlichte Reihen:

Auf der Inik-Seite (<http://www.informatik-im-kontext.de/>) veröffentlicht:

- [Chatbots](#) (Helmut Witten, Malte Hornung - Bln)

Right Sidebar:

- Create a page
- Upload files
- Invite more people
- Share this page
- Put this page in a folder
- Add Tags
- Control access to this page
- Copy this page

Navigator:

- Fallbeispiel 02 Planspiel Datenschutz 2_0
- FrontPage**
- Geschichte der Kommunikation
- Inik ohne Computer
- KompetenzenAudio
- Kompetenztabelle

Unterrichtsmaterial zu „Informatik im Kontext“?



- Informationen und Unterrichtsmaterial auf <http://informatik-im-kontext.de> veröffentlicht

The screenshot shows the website 'informatik im Kontext'. The header features the title 'INFORMATIK im Kontext' in a stylized font. Below the title is a navigation bar with links: 'Startseite', 'Konzepte', 'Entwürfe', 'Kontextideen', 'Pläne', and 'Kontakt'. The main content area is divided into two columns. The left column, highlighted in yellow, lists various topics under the heading 'Entwürfe:': 'Chatbots', 'Email nur für Dich', 'Bildverarbeitung', 'Filesharing', 'Faltblatt', 'Audiobearbeitung', 'Soziale Netze', and 'BEIN'. The right column, also highlighted in yellow, is titled 'Konzepte' and contains the following text: 'Auf dieser Seite werden grundlegende Beiträge veröffentlicht, sobald sie erstellt und gegengelesen wurden. Ein Konzeptpapier zu Informatik im Kontext ist in Vorbereitung und wird auf der INFOS 2009 vorgestellt. Eine Inspirationsquelle ist die Dokumentation zum Projekt Chemie im Kontext.' Below this, there is a section titled 'Vorträge' with three entries: 'Koubek: Informatik im Kontext. Vortrag beim Informatiklehrertag an der Universität Bayreuth 2010.', 'Koubek; Schulte; Schulze; Witten: Informatik im Kontext. Ein integratives Unterrichtskonzept für den Informatikunterricht. Vortrag auf der INFOS 2009.', and 'Koubek: Informatik im Kontext. Konzepte und Entwürfe. Vortrag anlässlich der Bundesfachleitertagung'.

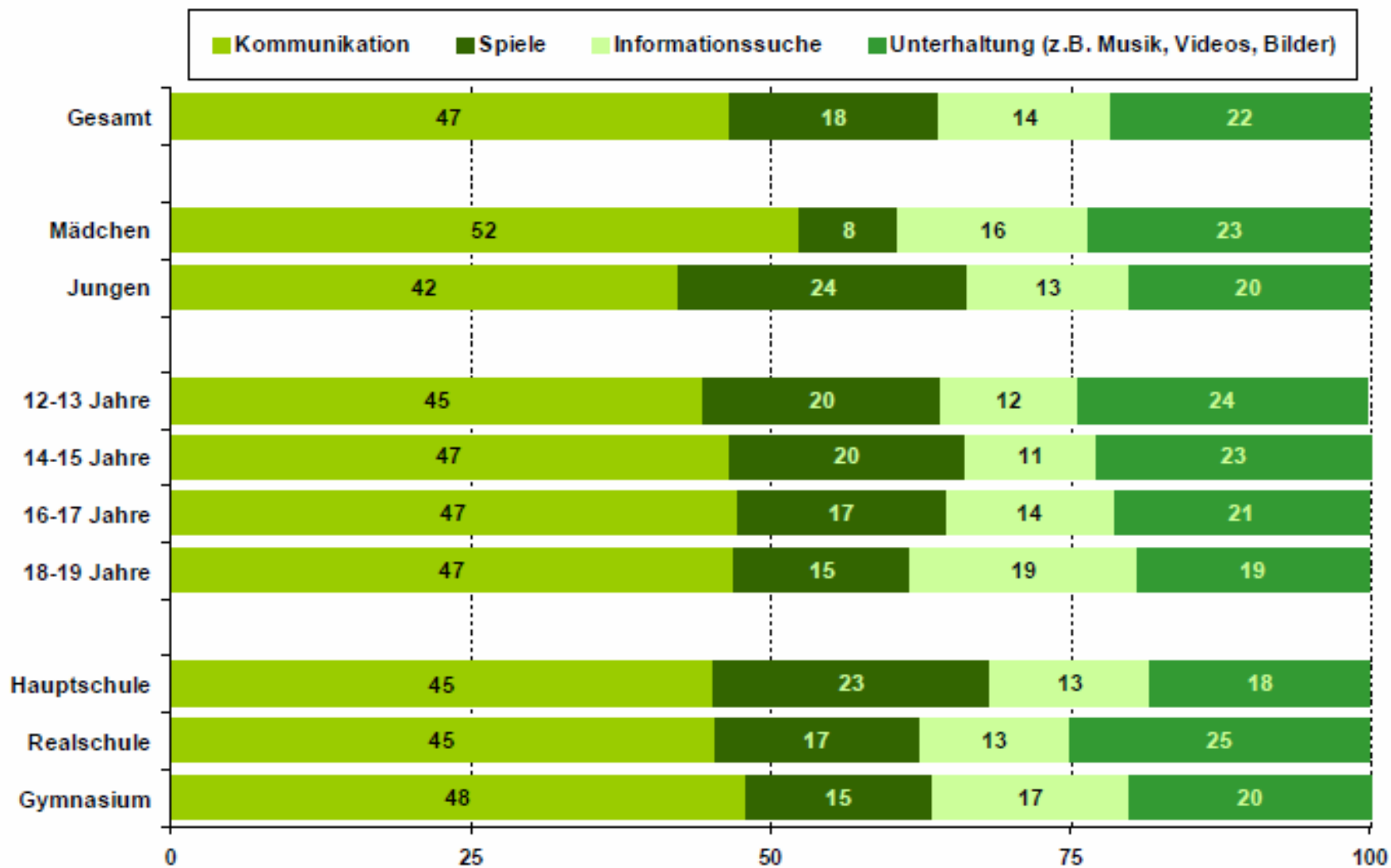
„Sichere Kommunikation über ein öffentliches Medium“



eine kontextorientierte Unterrichtsreihe zur kritischen Würdigung
der ***Revolution des Briefverkehrs*** im 20. Jahrhundert

- Kontext in der Lebenswelt der Schülerinnen und Schüler bedeutsam (sie kommunizieren täglich über das Internet)
- Konstruktion von Sicherheitsmechanismen erfordert fundierte Kenntnisse der Gefahren
- Realisierung von Sicherheitsmechanismen motiviert Anwendung mathematischer Verfahren

Inhaltliche Verteilung der Internetnutzung 2009

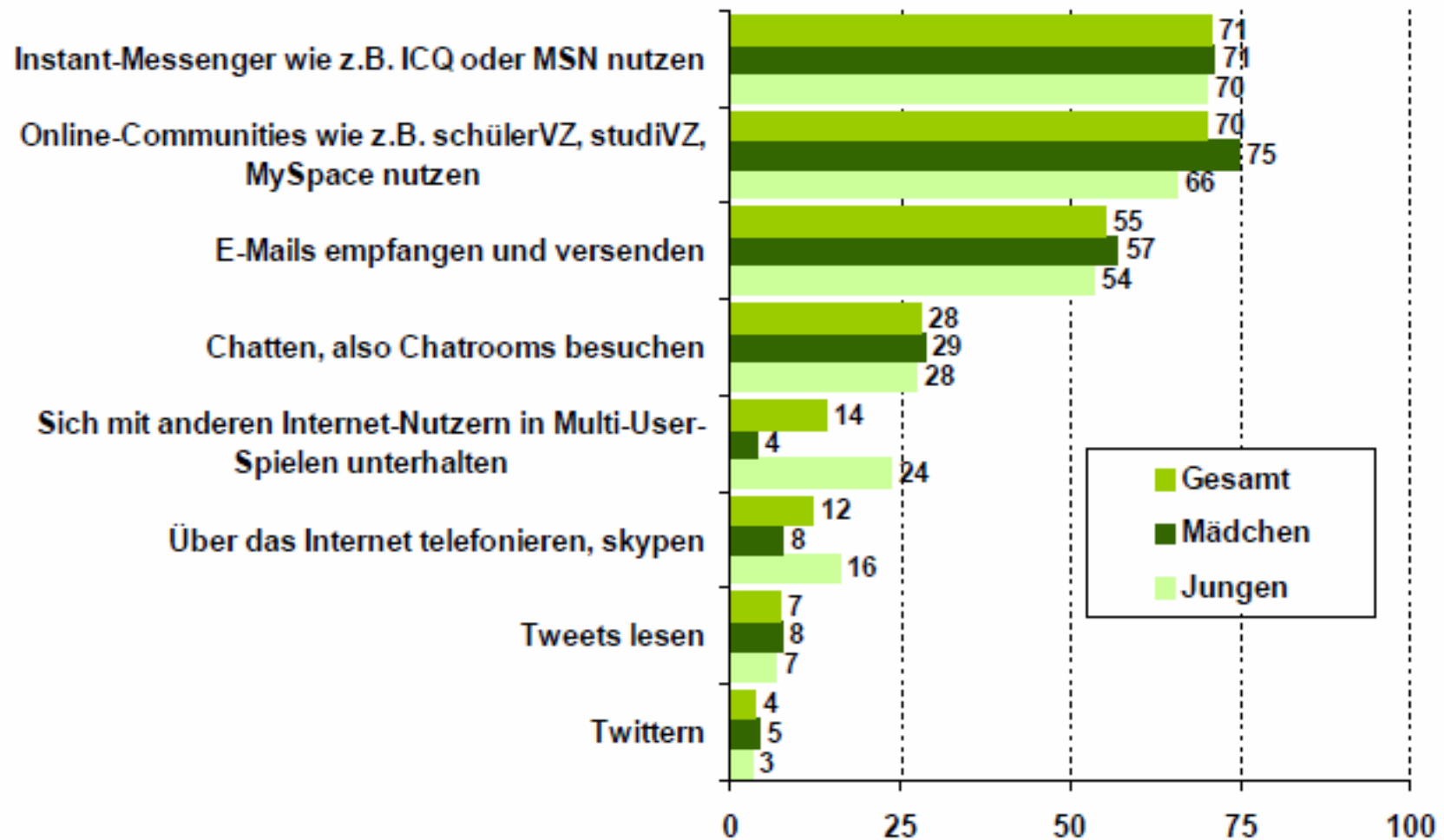


Quelle: JIM 2009, Angaben in Prozent

Basis: Internet-Nutzer, n=1.173

Aktivitäten im Internet – Schwerpunkt Kommunikation

- täglich/mehrmals pro Woche -



Quelle: JIM 2009, Angaben in Prozent

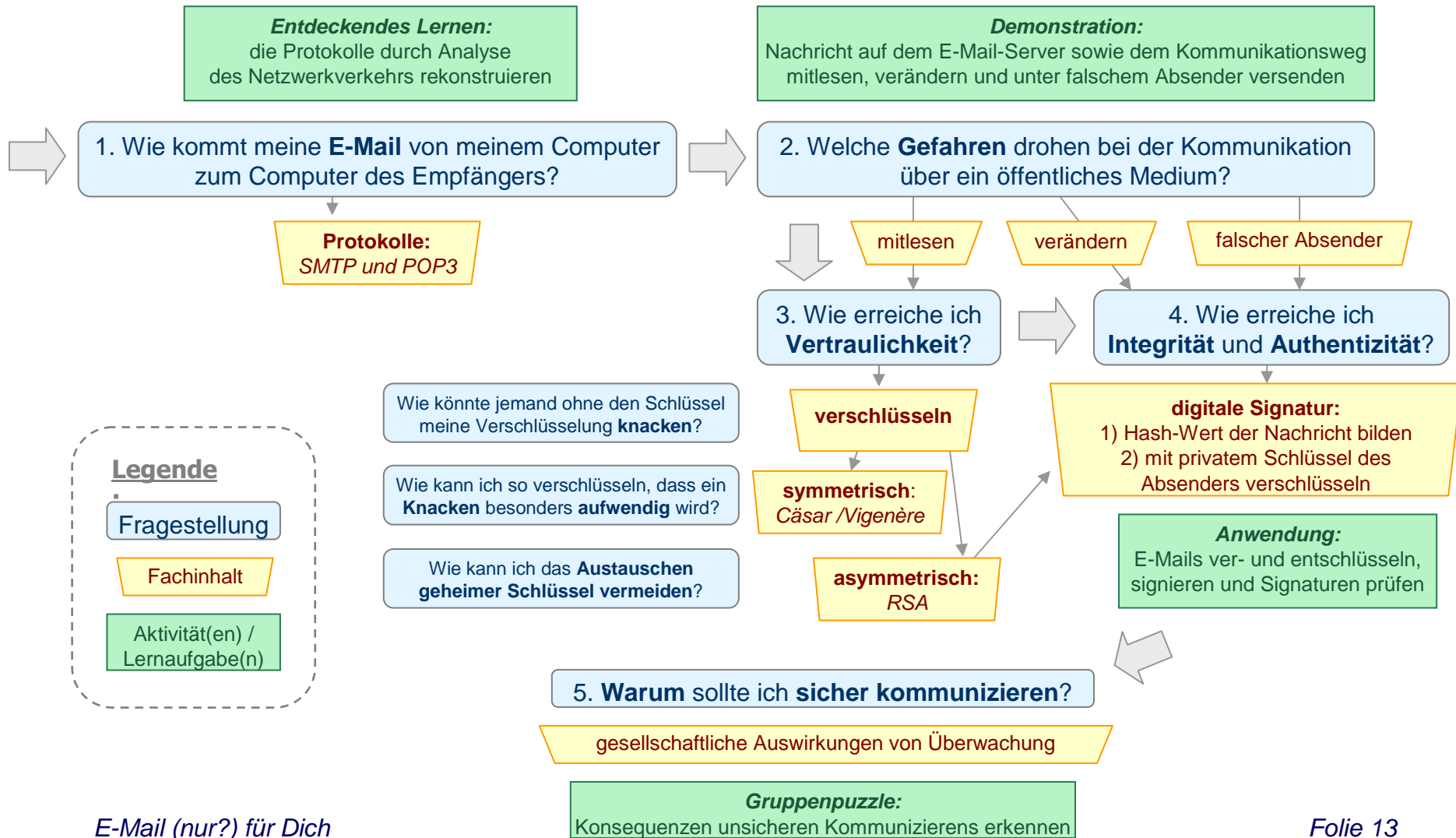
Basis: alle Befragten, n=1.200

Fragestellungen in diesem Kontext:



1. Wie kommt meine **E-Mail** von meinem Computer zum Computer des Empfängers?
2. Welche **Gefahren** drohen bei der Kommunikation über ein öffentliches Medium?
3. Wie erreiche ich **Vertraulichkeit**?
4. Wie erreiche ich **Integrität** und **Authentizität**?
5. **Warum** sollte ich **sicher kommunizieren**?

Verlauf des Lernprozesses

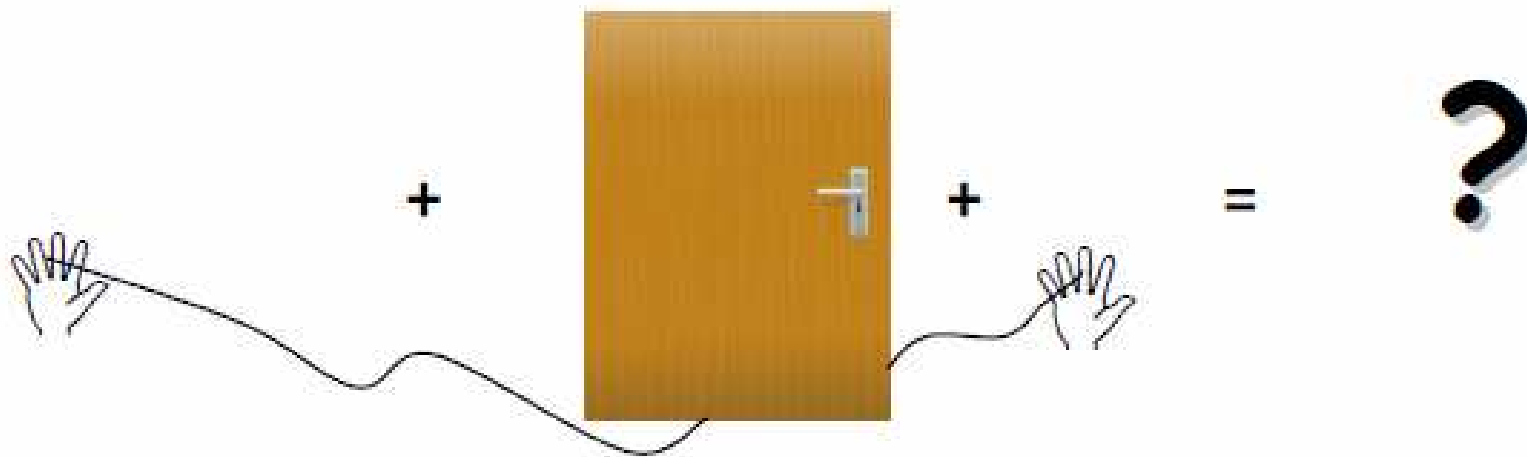


Schritt 1: E-Mail-Protokolle entdecken



- Konzept eines Protokolls erarbeiten
- Netzwerkverkehr eines E-Mail-Clientprogramms in Partnerarbeit analysieren
- Gemeinsamkeiten und Unterschiede benennen

Konzept eines E-Mail-Protokolls erarbeiten



Schritt 2: Gefahren bei der Kommunikation erkennen



Demonstration durch den Lehrer, Schülerinnen und Schüler notieren Beobachtungen und formulieren Anforderungen an eine sichere Kommunikation:

- Vortäuschen eines falschen Absenders (Einstellungen im Mail-Client)


Schritt 2: Gefahren bei der Kommunikation erkennen



Tip von Bundeskanzler - Thunderbird

Datei Bearbeiten Ansicht Navigation Nachricht OpenPGP Extras Hilfe

Abrufen Verfassen Adressbuch Entschlüsseln Antworten Allen antworten Weiterleiten Schlagwörter Löschen

 **Diese Nachricht könnte ein Betrugsversuch (Phishing) sein.** Kein Betrug

Betreff: Tip von Bundeskanzler
Von: [Angela Merkel <bundeskanzlerin@bund.de>](mailto:angela.merkel@bundeskanzlerin.de)
Antwort an: bundeskanzlerin@bund.de
Datum: 13.09.2010 09:46
An: bruno@r011-l1, henning@r011-l1, leon@r011-l1, karim@r011-l1, sahana@r011-l1, samir@r011-l1, dennis@r011-l1

Mein lieber Freund,

als Bundeskanzler verfüge ich über mehr Information als normale Einwohner. Ich gebe dir Tip: Kaufe jetzt Aktien von Gatsprom unter <http://www.gazprom.com> befor Deutsche Firma RWE übernimmt!!!

Viele Grusse,

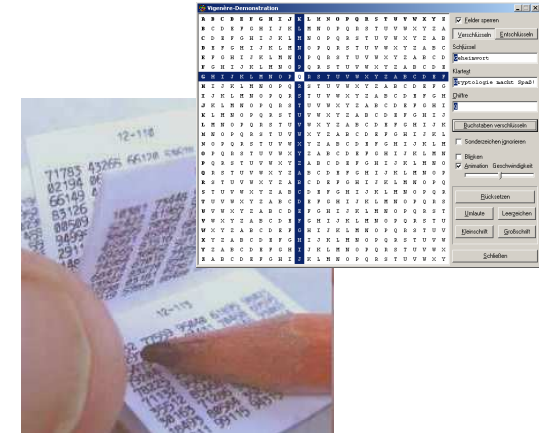
Angela Merckel

Schritt 3: Verschlüsselung

Wiederholt werden Verfahren erarbeitet und ihre Sicherheit durch Knacken ohne Schlüssel kritisch hinterfragt:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- Caesar
- Vigenère und One-Time-PAD
- RSA



Schritt 4: Digitale Unterschrift



- Animation zum Prinzip der Digitalen Unterschrift
- Schlüssel erzeugen und austauschen und damit E-Mails verschlüsseln und digital unterschreiben
- Verschlüsselte Nachrichten im Netzwerk-analysewerkzeug betrachten

Alice Computer

Internet

Bobs Computer

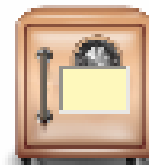
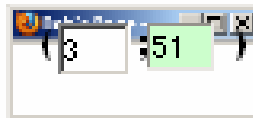
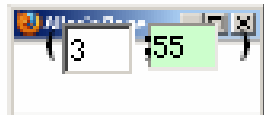


privater Schlüssel:

öffentlicher Schlüssel:

öffentlicher Schlüssel:

privater Schlüssel:



anzuwendender Schlüssel:



anzuwendender Schlüssel:



streng geheim

'ybolmtmogon4

'ybolmtmogon4

Schlüssel auf Nachricht anwenden

Schlüssel auf Nachricht anwenden

19,20,18,5,14,7,32,7,5,8,5,9,13



39,25,2,15,49,13,43,13,15,17,15,14,52

Hashwert 2



Signatur 2

Schlüssel auf Signatur anwenden

2 Hashwert



8 Signatur

Schlüssel auf Signatur anwenden



Schritt 5: Gründe für eine sichere Kommunikation



Gruppenpuzzle zu folgenden Themen:

- Informationsfreiheit
- Pretty Good Privacy (PGP)
- De-Mail
- Echolon



Fazit



Die Schülerinnen und Schüler ...

- ... erleben Kryptographie in einem sinnstiftenden Zusammenhang
- ... entwickeln ein fundiertes Bewusstsein für Sicherheitsaspekte beim Einsatz von Computersystemen
- ... erarbeiten sich eigenständig intelligent vernetztes Wissen und Strategien

Kritik / Perspektive

- Wo bleiben die Fachinhalte?
 - Curricula beim Einsatz der Reihe berücksichtigen, z.B. Themen Netzwerke, Computersicherheit, Kryptologie
 - Schwerpunkte dieser Reihe:
 - Inhaltsbereich Informatiksysteme
 - Inhaltsbereich Informatik, Mensch und Gesellschaft
 - Prozessbereich Begründen und Bewerten
- Muss ich denn gleich min. 19 Stunden planen?
 - Modularisierung geplant
- Wo bleibt die Programmierung?
 - Rahmenwerk mit Musterimplementierungen für Java, Python und Delphi geplant

Vielen Dank für Ihre Aufmerksamkeit!

Quelle JIM Studie:

<http://www.mpfs.de/fileadmin/JIM-pdf09/JIM-Studie2009.pdf>

Bildquelle One-Time-Pad:

<http://users.telenet.be/d.rijmenants/pics/otpbooklet1.jpg>