




Back to
SCHOOL

Sicher kommunizieren und verschlüsseln

Eric Schreiber

Motivation

CC BY Tino Hempel



HANSE-MENÜ
Service GmbH Rostock

Tel.: 0381 77691-20
0381 77691-22 (mit Anrufbeantworter)

Hanse-Menü-Service GmbH

Kundenlogin:
Kundennummer:

Passwort:

[Schon registriert?](#)

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---------------------------------|
| 67 | 7.892216 | 192.168.178.32 | 188.68.32.174 | HTTP | 762 | POST /?ear_a=akt_login HTTP/1.1 |
| 69 | 8.014439 | 188.68.32.174 | 192.168.178.32 | HTTP | 1506 | HTTP/1.1 200 OK |
| 70 | 8.025104 | 188.68.32.174 | 192.168.178.32 | HTTP | 1506 | Continuation |

▶ Frame 67: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface 0

▶ Ethernet II, Src: IntelCor_76:74:92 (00:26:c6:76:74:92), Dst: Avm_a9:d9:72 (34:81:c4:a9:d9:72)

▶ Internet Protocol Version 4, Src: 192.168.178.32, Dst: 188.68.32.174

▶ Transmission Control Protocol, Src Port: 12314, Dst Port: 80, Seq: 1, Ack: 1, Len: 708

▶ **Hypertext Transfer Protocol**

▲ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "Login_Name" = "140033"
- ▶ Form item: "Login_Passwort" = "4711"

Agenda

01

Curriculare Vorgaben

Welche Vorgaben sind vorgeschrieben und wo finde ich diese?

02

Kurzer inhaltlicher Input

Grundlagen, wichtige Begriffe

03

Praktische Umsetzung

Inhalte

04

Zusammenfassung und Ausblick



Curriculare Vorgaben

Der (neue) Rahmenplan

Rahmenplan Klasse 7

Sicher kommunizieren und kooperieren – 8 Unterrichtsstunden

Die Schülerinnen und Schüler verschlüsseln Daten und tauschen diese aus. Sie lernen anhand historischer Verfahren das Prinzip der symmetrischen Verschlüsselung kennen. Sie begründen die Notwendigkeit für Sicherung der Vertraulichkeit und wenden das Prinzip auf Dokumente und bei der Informationsübertragung an.

| Ziele | Hinweise und Bezüge |
|---|---|
| klassische Verfahren der symmetrischen Verschlüsselung erläutern und anwenden REAKTIVIERBAR | Die Schülerinnen und Schüler beschreiben klassische Verfahren unter Verwendung der Begriffe Klartext- und Geheimtextalphabet, Klartext und Geheimtext, Schlüssel, Verschlüsseln und Entschlüsseln. Die Schülerinnen und Schüler argumentieren zur Sicherheit der Verfahren. |

Rahmenplan Klasse 7

| Ziele | Hinweise und Bezüge |
|--|---|
| Softwarelösungen zur Verschlüsselung nutzen SICHER | <p>Mögliche Lösungen sind das Verschlüsseln von Daten mit internen Programmfunktionen oder mit eigenständigen Programmen.</p> <p>Die Schülerinnen und Schüler achten auf die Verwendung von Kommunikationsprotokollen, die eine Komponente zur Verschlüsselung der Daten beinhalten.</p> <p>Die Schülerinnen und Schüler sind in der Lage, verschlüsselte Daten als E-Mail-Anhang zu versenden.</p> <p>➤ Jahrgangsstufe 6: In der vernetzten Welt kommunizieren</p> |
| Merkmale sicherer Kennwörter begründen SICHER | <p>Bei der Wahl sicherer Kennwörter beachten die Schülerinnen und Schüler sowohl technische als auch psychologische Aspekte.</p> |

Rahmenplan Klasse 9

Daten zuverlässig und korrekt übertragen – 6 Unterrichtsstunden

Die Schülerinnen und Schüler lernen Verfahren kennen, mit deren Hilfe Daten auf Korrektheit geprüft und sicher übertragen werden können. Mit der asymmetrischen Verschlüsselung lernen sie ein Prinzip kennen, das die Nachteile der symmetrischen Verschlüsselung ausgleicht.

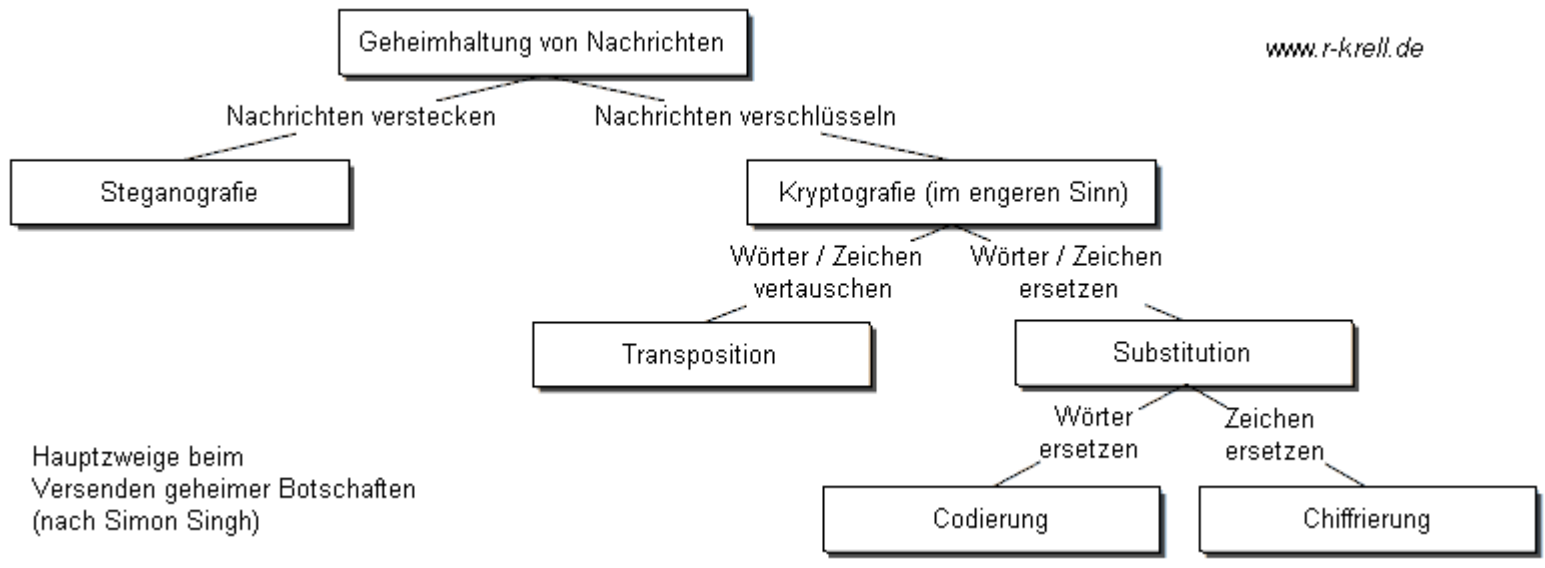
das Prinzip der asymmetrischen Verschlüsselung beschreiben

EXEMPLARISCH

Die Schülerinnen und Schüler erkennen, dass die Verwendung eines Paares aus privatem und öffentlichem Schlüssel den Nachteil der symmetrischen Verschlüsselung – den geheimen Austausch eines gemeinsamen Schlüssels über eine öffentliche Verbindung – aufhebt. Das Prinzip sollte anschaulich und ohne die Durchführung komplexer Berechnungen demonstriert werden.

Gesamtübersicht

www.r-krell.de



Quelle: <http://www.r-krell.de/if-java-j.htm> (aufgerufen am 20.08.2018)



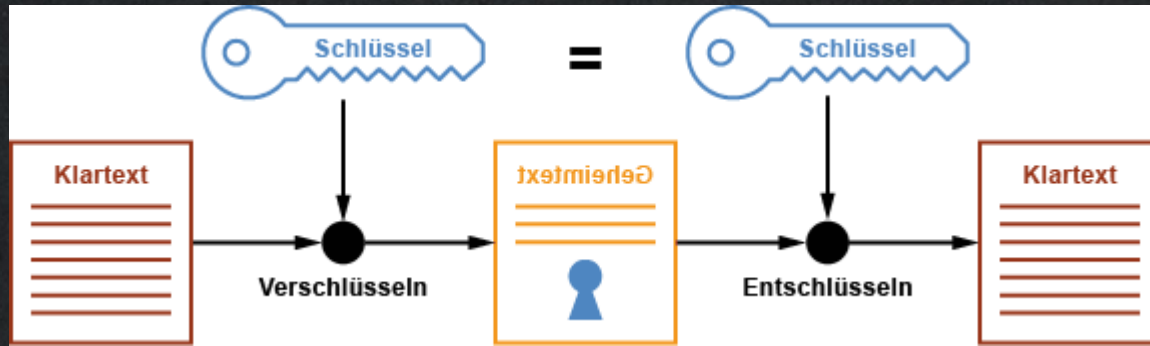
Praktische Umsetzung

Inhalte

Grundlagen der Verschlüsselung

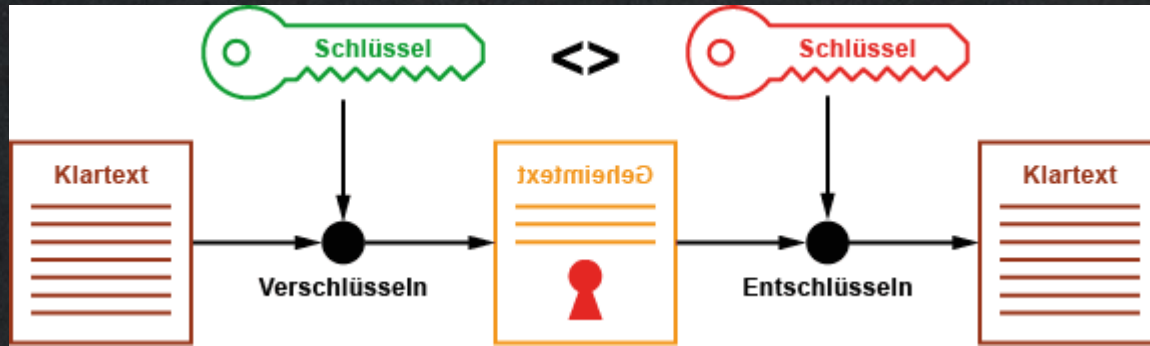


Symmetrische Verschlüsselung



Quelle: <https://www.elektronik-kompodium.de/sites/net/1907041.htm> (aufgerufen am 20.08.2018)

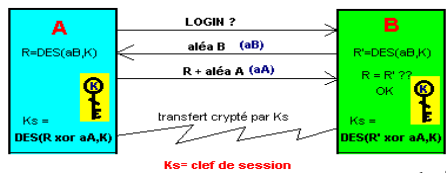
Asymmetrische Verschlüsselung



Quelle: <https://www.elektronik-kompodium.de/sites/net/1907041.htm> (aufgerufen am 20.08.2018)

Geheime Kommunikation von 1950 bis heute

© Witten, 2003



symétrisch
(geheimer Schlüssel)

Blockchiffrier-
algorithmen

DES (Feistel)



Stromchiffrier-
algorithmen

XOR - RC4 (WEP, WPA)
(Rivest)



moderne computergestützte
Verfahren

asymmetrisch
(Public Key, Diffie u. Hellmann)



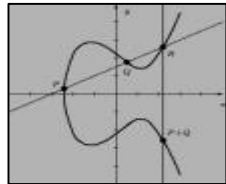
RSA
(Rivest, Shamir, Adleman)



El Gamal



Elliptische Kurv
en



A rectangular chalkboard with a light-colored wooden frame is positioned diagonally on a background of vertical wooden planks. The planks have a weathered, rustic appearance with varying shades of brown and grey. The chalkboard itself is black and contains the text 'Vielen Dank' in a clean, white, sans-serif font, centered horizontally and vertically.

Vielen Dank