Sicher kommunizieren und verschlüsseln

Eric Schreiber

Agenda

01 **Curriculare Vorgaben**
Welche Vorgaben sind vorgeschrieben und wo finde ich diese?

02 **Kurzer inhaltlicher Input**
Grundlagen, wichtige Begriffe

03 **Praktische Umsetzung**
Welche Inhalte und welche Methoden?

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

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

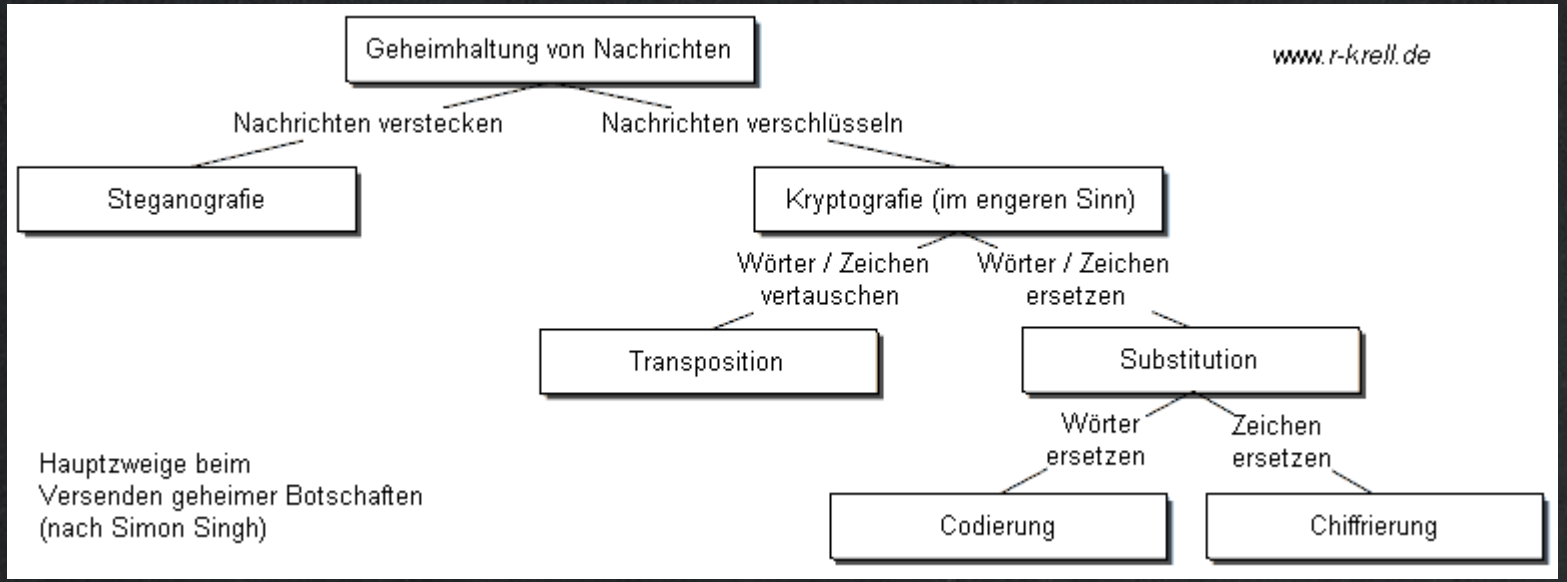
das Prinzip der asymmetrischen Verschlüsselung beschreiben **EXEMPLARISCH**	Die Schülerinnen und Schüler erkennen, dass die Verwendung eines Paares aus privatem und öffentlichem Schlüssel den Nachteil der symmetrischen Verschlüsselung – den geheimen Austausch eines gemeinsamen Schlüssels über eine öffentliche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

Praktische Umsetzung

Inhalte

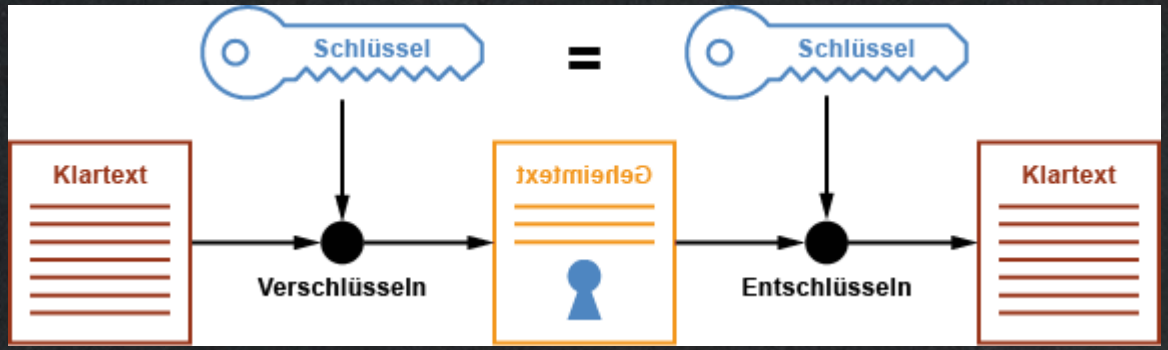
Grundlagen der Verschlüsselung

Gesamtübersicht



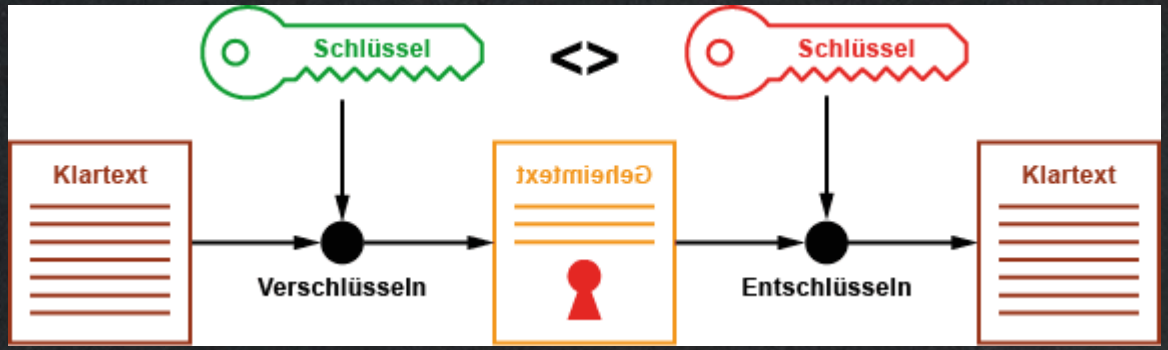
Quelle: http://www.r-krell.de/if-java-j.htm (aufgerufen am 20.08.2018)

Symmetrische Verschlüsselung



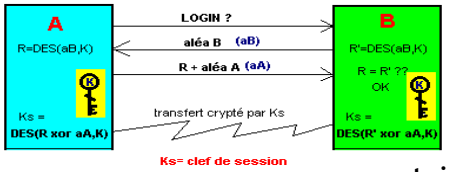
Quelle: https://www.elektronik-kompendium.de/sites/net/1907041.htm (aufgerufen am 20.08.2018)

Asymmetrische Verschlüsselung



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

Geheime Kommunikation
von 1950 bis heute



moderne computergestützte Verfahren

symmetrisch
(geheimer Schlüssel)

asymmetrisch
(Public Key, Diffie u. Hellmann)

Blockchiffrier-algorithmen

Stromchiffrier-algorithmen

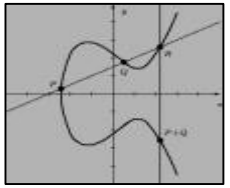
DES (Feistel)

XOR - RC4 (WEP, WPA)
(Rivest)

RSA
(Rivest, Shamir, Adleman)

El Gamal

Elliptische Kurven




Vielen Dank