11/12.F2 Sichere Kommunikation

Rahmenplan

Sichere Kommunikation [MD2] [MD4] [DRF] **ca. 9/14 Unterrichtsstunden**

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
Aspekte der Kryptologie • Kommunikation mithilfe von Sequenzdiagrammen interpretieren und darstellen • die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen • die Sicherheit kryptografischer Verfahren mithilfe des Prinzips von Kerckhoffs prüfen • das Prinzip der asymmetrischen Verschlüsselung erläutern • die Prinzipien digital zertifizierter und signierter Daten erläutern • die Grenzen der modernen Kryptografie anhand der Einwegfunktionen erläutern [MD6]	Die Behandlung des Themas erfolgt anschaulich und ohne umfangreiche mathematische Berechnungen. Dazu können mono- und polyalphabetische Verschlüsselungsverfahren analysiert werden. Das One-Time-Pad ist als einzig sicheres Verfahren zu thematisieren. Das Prinzip der Einwegfunktion ist anschaulich darzustellen. Die Sicherheit der modernen Kryptografie beruht auf der Annahme, dass keine effizienten Verfahren für die Umkehrung der Einwegfunktionen existieren. Die Sicherheit kann weiterhin anhand der Ineffizienz von Brute-Force-Verfahren gezeigt werden.

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Rahmenplan-Spirale

Sicher kommunizieren

Verbindliche Ziele und Inhalte

Klasse 7

Verschlüsselung verstehen

- klassische Verfahren der symmetrischen Verschlüsselung anschaulich erläutern

Prinzipien der Datenübertragung verstehen

Klasse 9

Verbindliche Ziele und Inhalte

grundlegende Prinzipien der Datenübertragung im Internet beschreiben

- Prinzip der asymmetrischen Verschlüsselung

autonom oder integrativ?

aktuell

- kaum Vorkenntnisse aus SI
- Thema in einem gesonderten Unterrichtsabschnitt sinnvoll

zukünftig

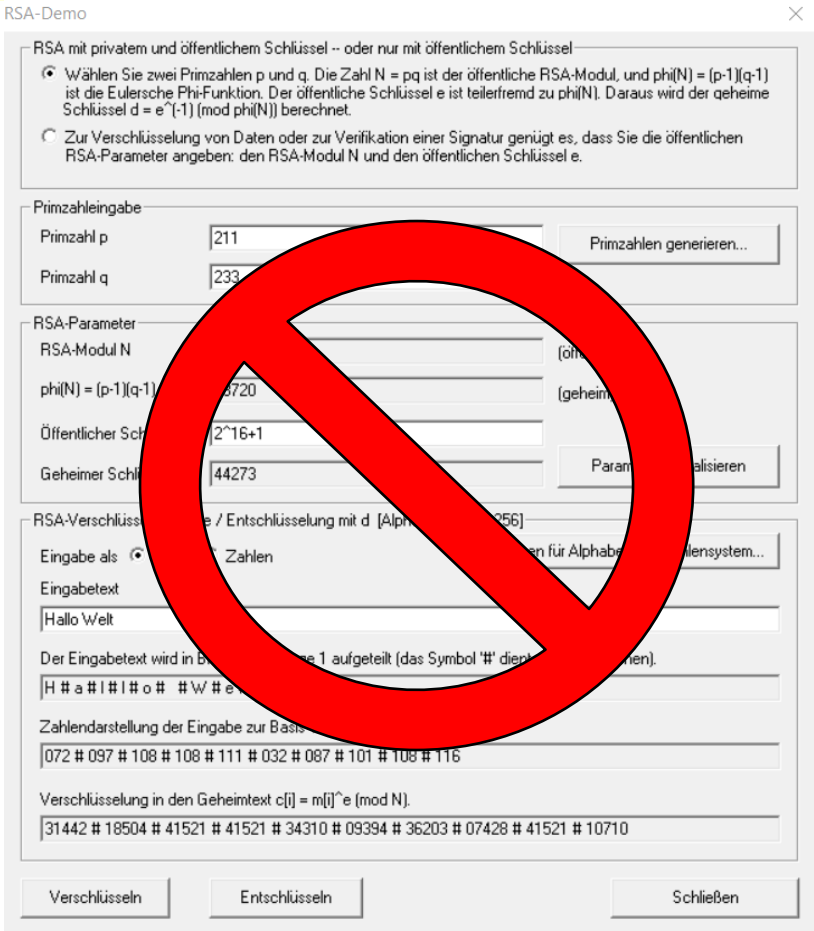
- Thema in Jg. 7 und 9 gemäß Spiralprinzip behandelt
- Wiederholung und Vertiefung des Wissens und Könnens
- Thema integrativ in Kontexte der Themen „Relationale Datenbanksysteme“, „Algorithmen und Daten“ oder „Kommunikation in vernetzten Systemen“ sinnvoll

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Wie/Was nicht?

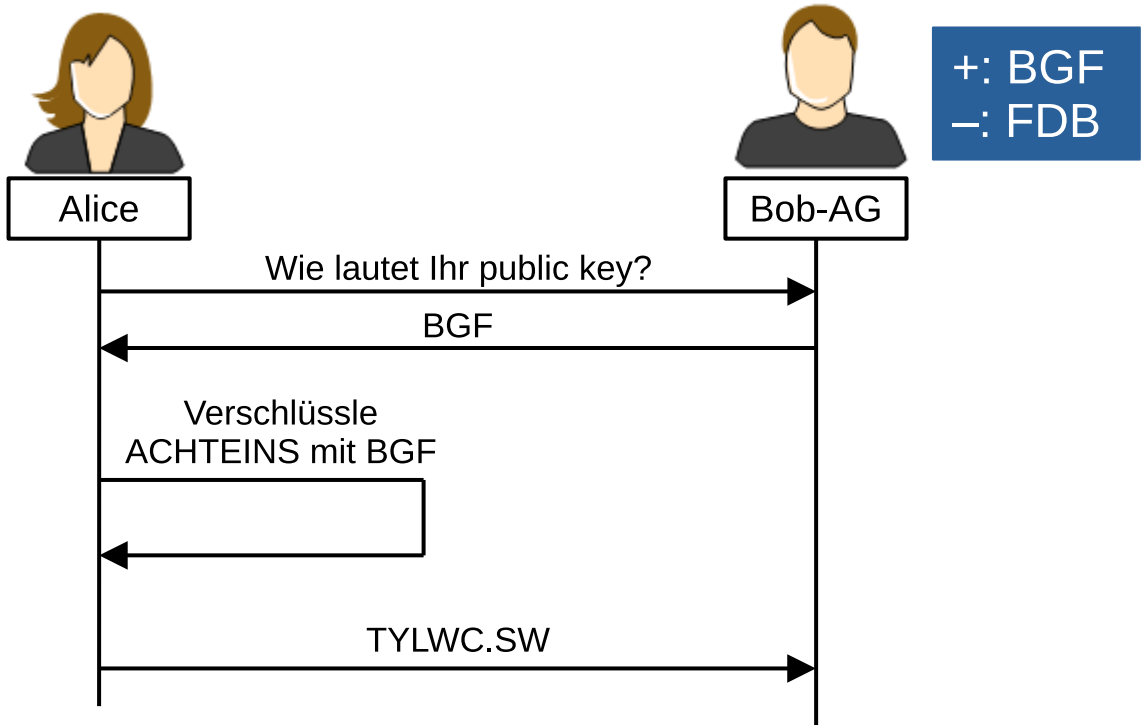
- umfangreiche mathematische Berechnungen
- vollständige Darstellung aller bekannten Verfahren
- alles implementieren



Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Vertiefung/Anwendung des Gelernten aus den Themengebieten „Vernetzte Systeme“ und „Softwareentwicklung“

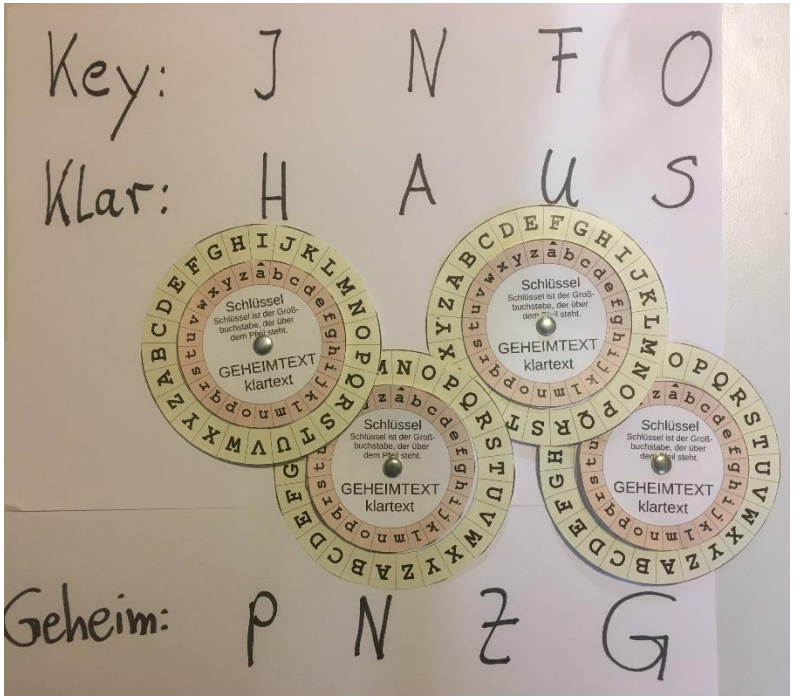


Anschaulichkeit

Die Behandlung des Themas erfolgt anschaulich und ohne umfangreiche mathematische Berechnungen.

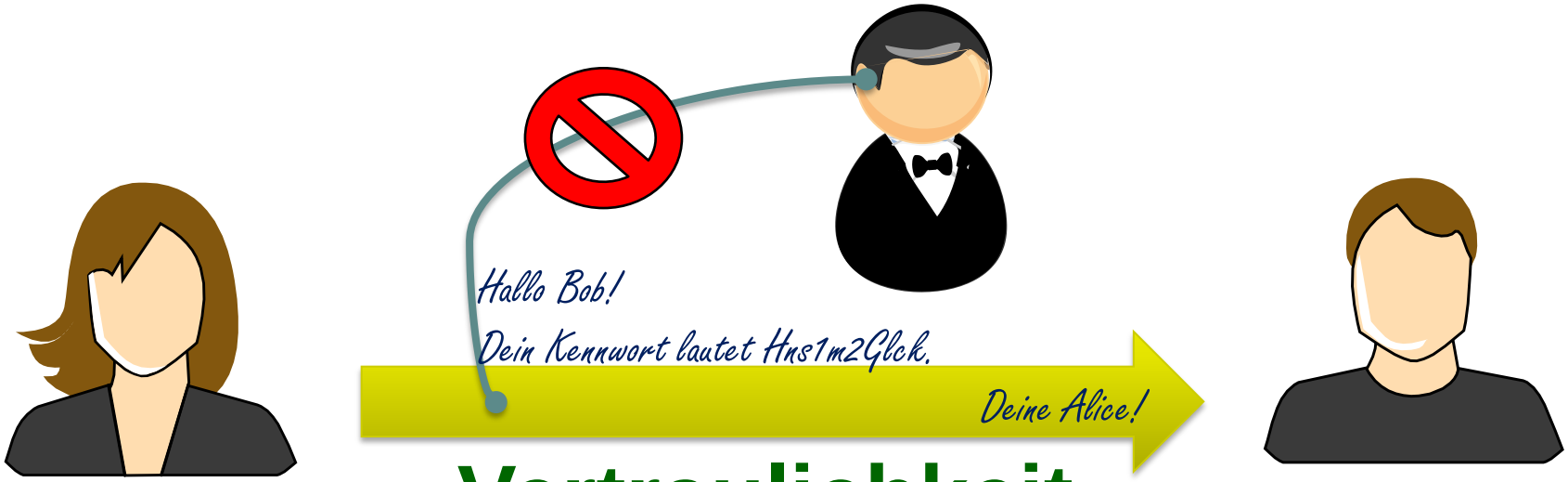
Ein Pfund Gehacktes

Wissen macht Ah! | 03.01.2019 | 24:41 Min. | Verfügbar bis 03.01.2024 | KiKa



Sicherheitsziele

- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen



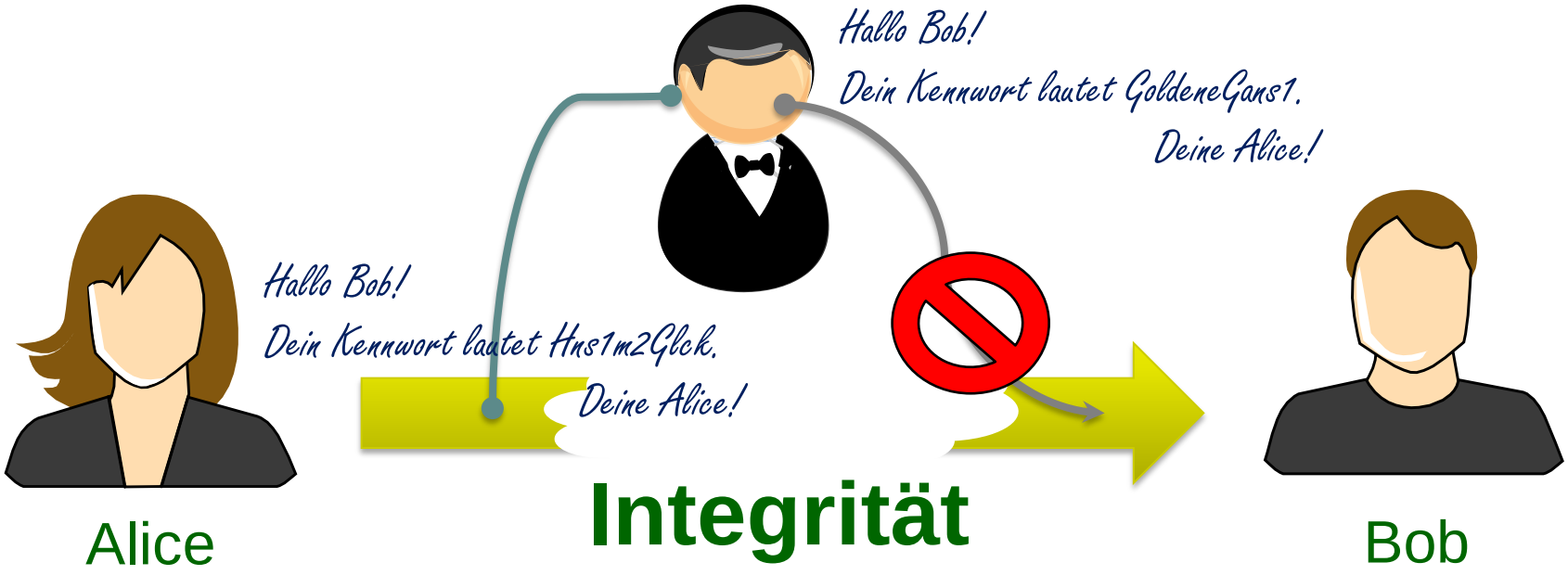
Vertraulichkeit

kein Mitlesen durch Fremde

Verschlüsselung

Sicherheitsziele

- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen



Integrität

keine Manipulation durch Fremde

Prüfziffern/Hash/Zertifikat

Sicherheitsziele

- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen

Authentizität

Nachricht ist definitiv vom Absender

Digitale Unterschrift

Sicherheitsziele

- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen

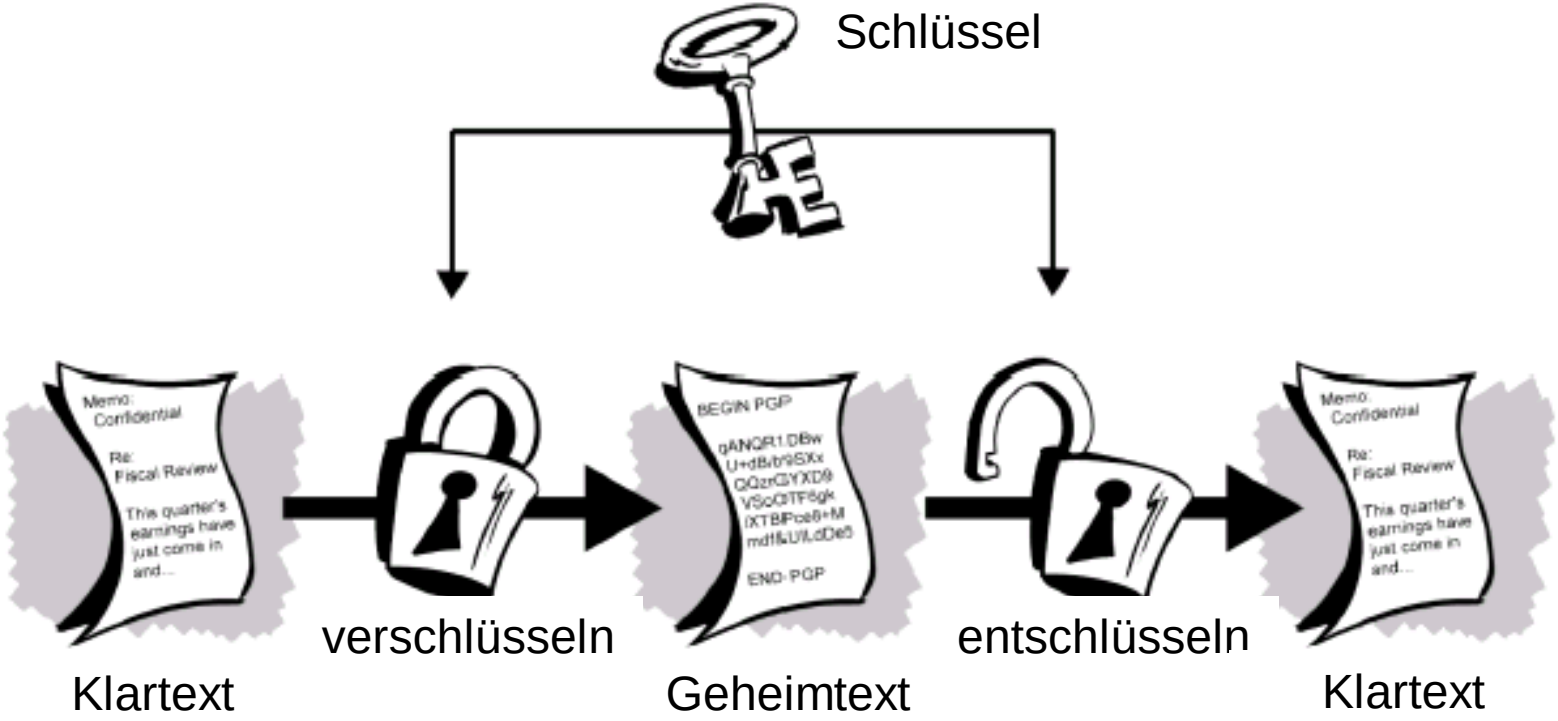
Verbindlichkeit

Keiner kann seine Urheberschaft bestreiten

Hash/Fingerprint/Signatur

Verfahren

Dazu können mono- und poly-alphabetische Verschlüsselungsverfahren analysiert werden.



aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.

Verfahren

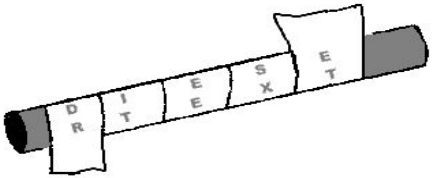
Dazu können mono- und poly-alphabetische Verschlüsselungsverfahren analysiert werden.

Steganographie
verstecken

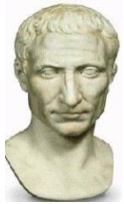
Kryptografie
verschlüsseln

Substitution
Zeichen/Wörter ersetzen

Transposition
Zeichen/Wörter umsortieren



Monoalphabetisch
Sherlock Holmes, Caesar



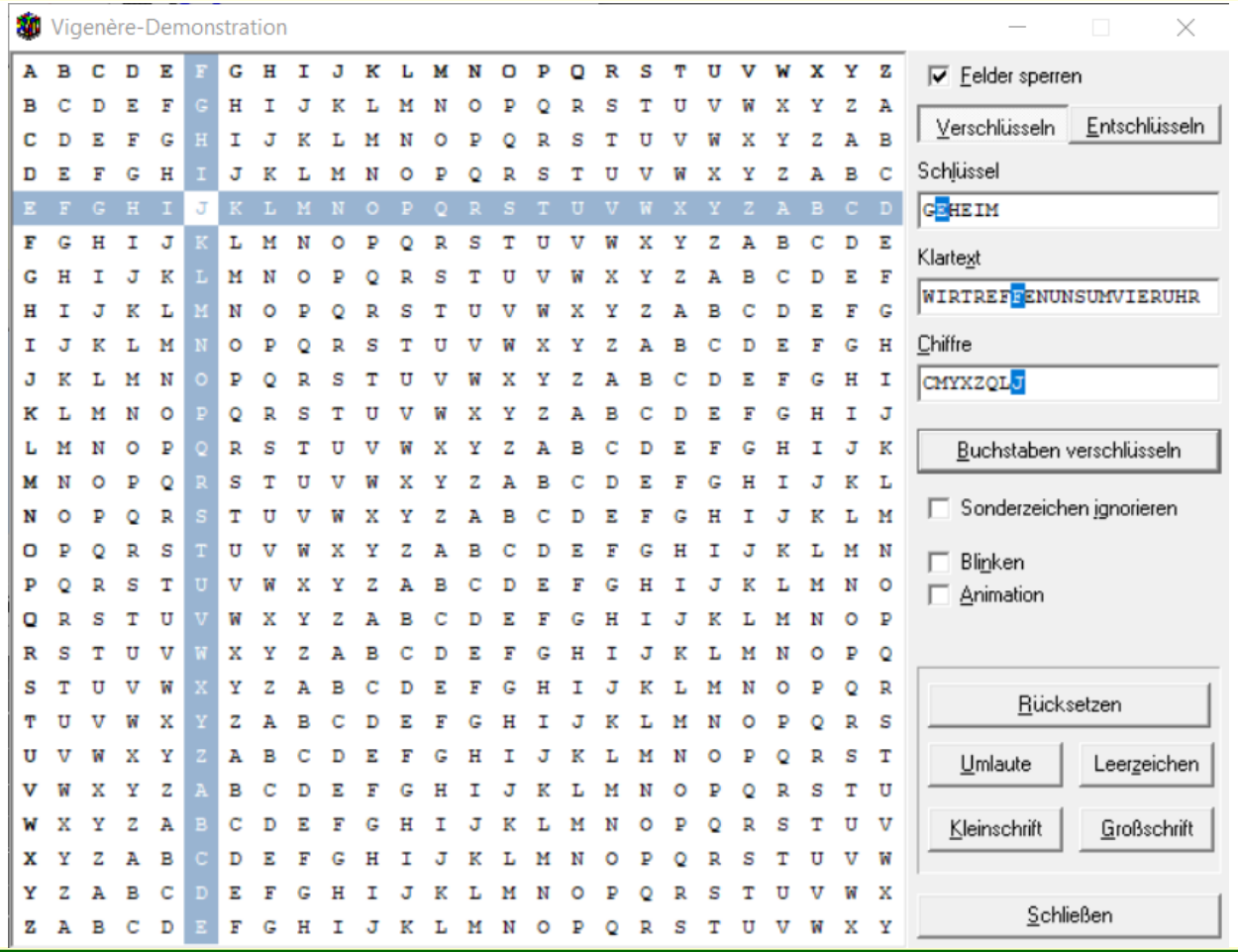
Polyalphabetisch
Vigenère, Enigma

One Time Pad

nach Witten, 2003

Vigenère-Verfahren

Dazu können mono- und poly-alphabetische Verschlüsselungsverfahren analysiert werden.

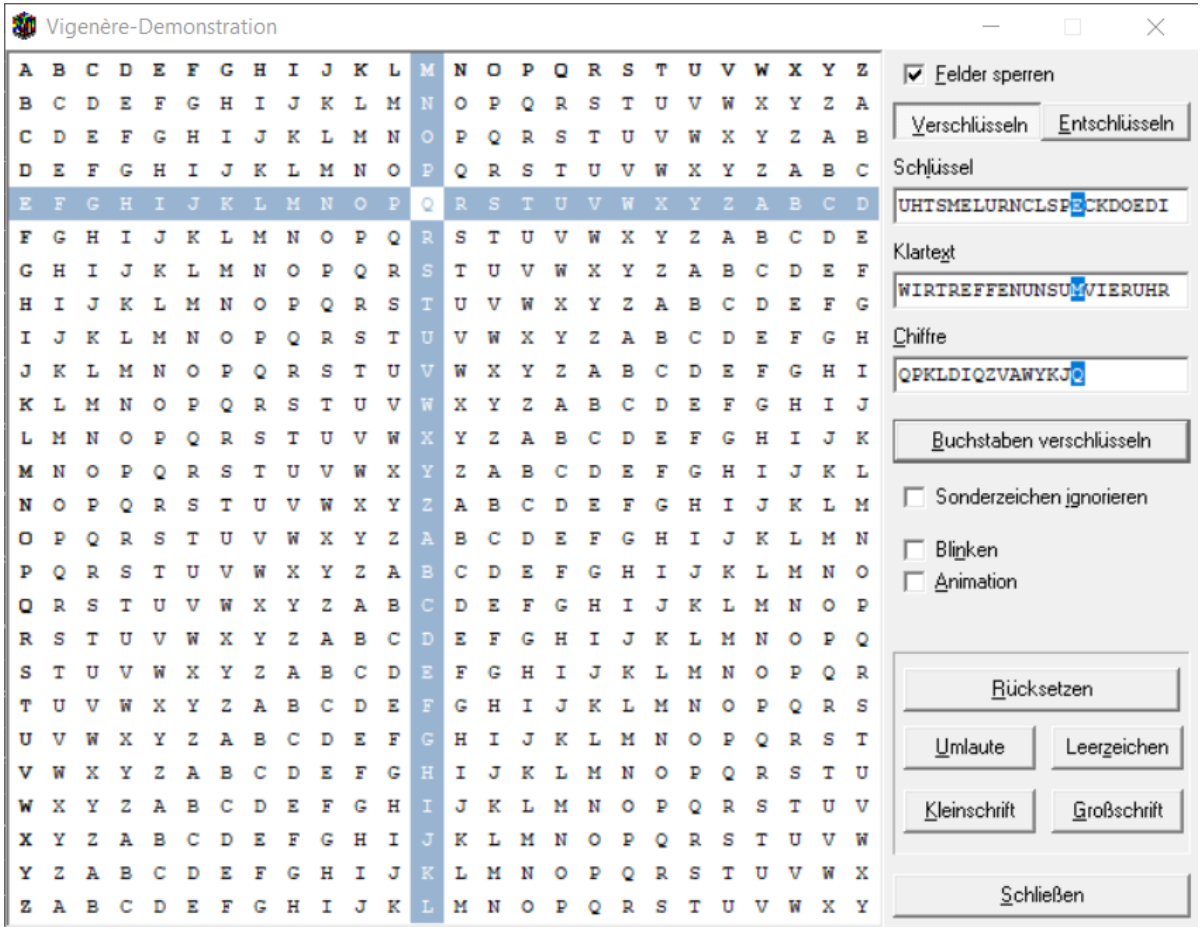


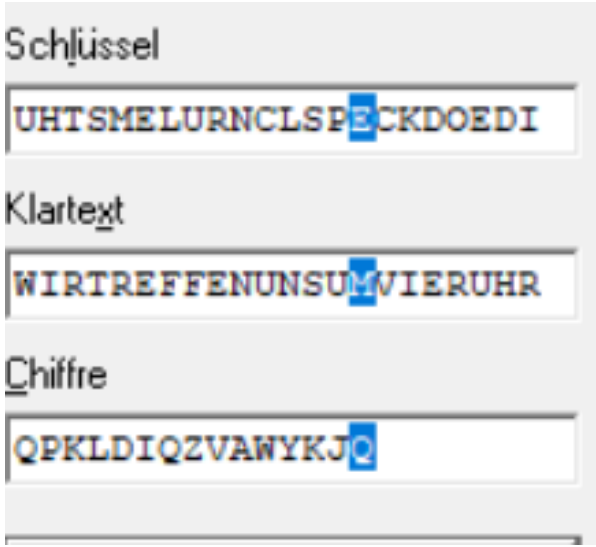
- polyalphabetisches Verfahren
- symmetrisches Verfahren

- Tool zur Erarbeitung: Krypto

One-Time-Pad

Das One-Time-Pad ist als einzig sicheres Verfahren zu thematisieren.





- Klartextlänge = Schlüssellänge
- Schlüssel zufällig
- Schlüssel nur 1x verwenden

One-Time-Pad

Das One-Time-Pad ist als einzig sicheres Verfahren zu thematisieren.

Aufgabe: Der Geheimtext MHOAYU wurde mit dem VIGENÈRE-Verfahren verschlüsselt.

a) Zeige, dass sich sowohl der Klartext SCHULE als auch der Klartext PAUSEN in den Geheimtext überführen lassen.

b) Ermittle einen weiteren, sinnvollen Klartext, der sich aus dem Geheimtext rekonstruieren lässt.

c) Leite eine Schlussfolgerung zur Sicherheit des VIGENÈRE-Verfahrens ab, wenn ein Schlüssel verwendet wird, der die gleiche Länge wie der Klartext hat.

Kerkhoffs Prinzip

- die Sicherheit kryptografischer Verfahren mithilfe des Prinzips von Kerckhoffs prüfen

Das **Verfahren** muss im Wesentlichen unentzifferbar sein und darf keine Geheimhaltung erfordern.

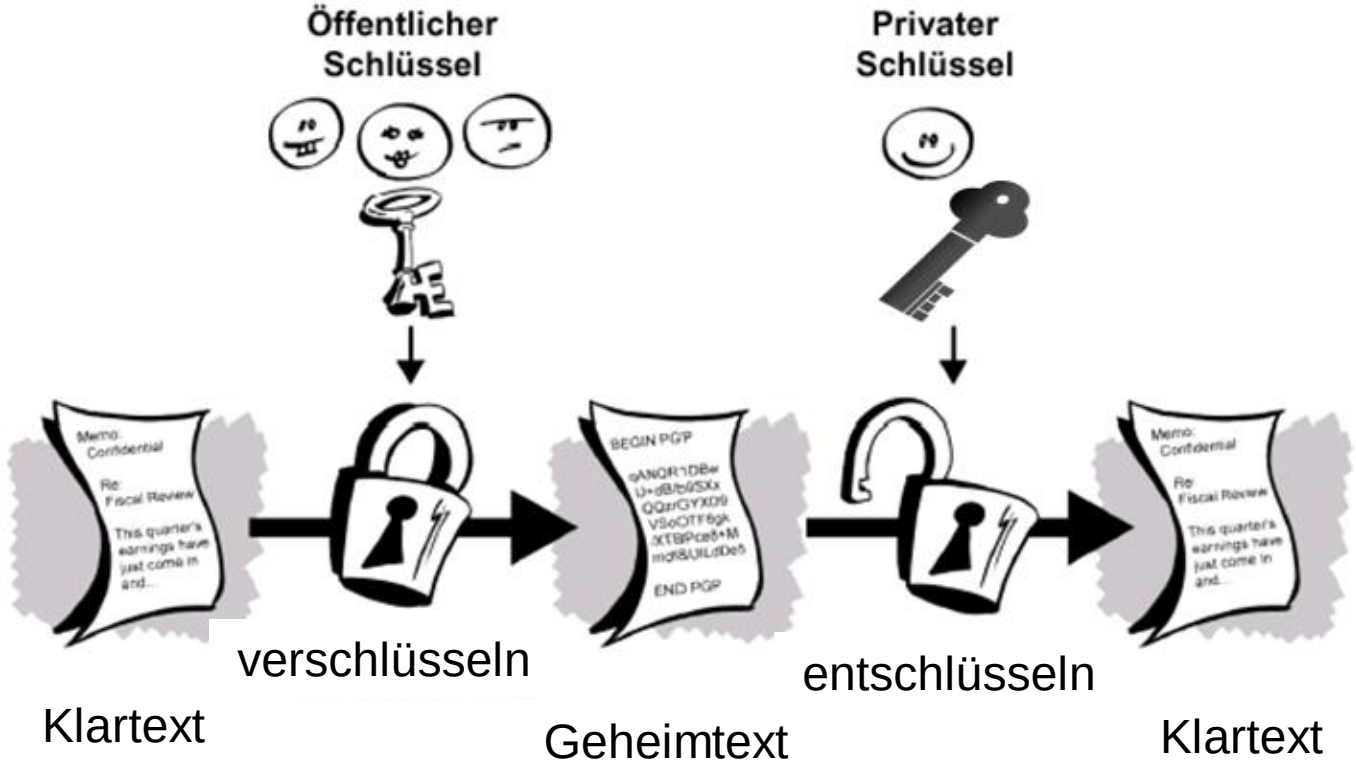
Die **Schlüssel** bedürfen weiterhin der Geheimhaltung.

Eugen Drezen, Historio de la Mondo Lingvo (Leipzig, 1931), 102

- Es ist schwieriger, ein kompromittiertes Verfahren zu ersetzen als einen kompromittierten Schlüssel.
- Es ist möglich, ein geheimes Verfahren durch Reverse Engineering zu rekonstruieren.
- Es ist leichter, Fehler/Hintertüren im Verfahren zu entdecken, wenn dieses öffentlich untersucht wird.
- Es ist leichter, in geheimen Verfahren Hintertüren zu verstecken.

Asym. Verfahren

- das Prinzip der asymmetrischen Verschlüsselung erläutern

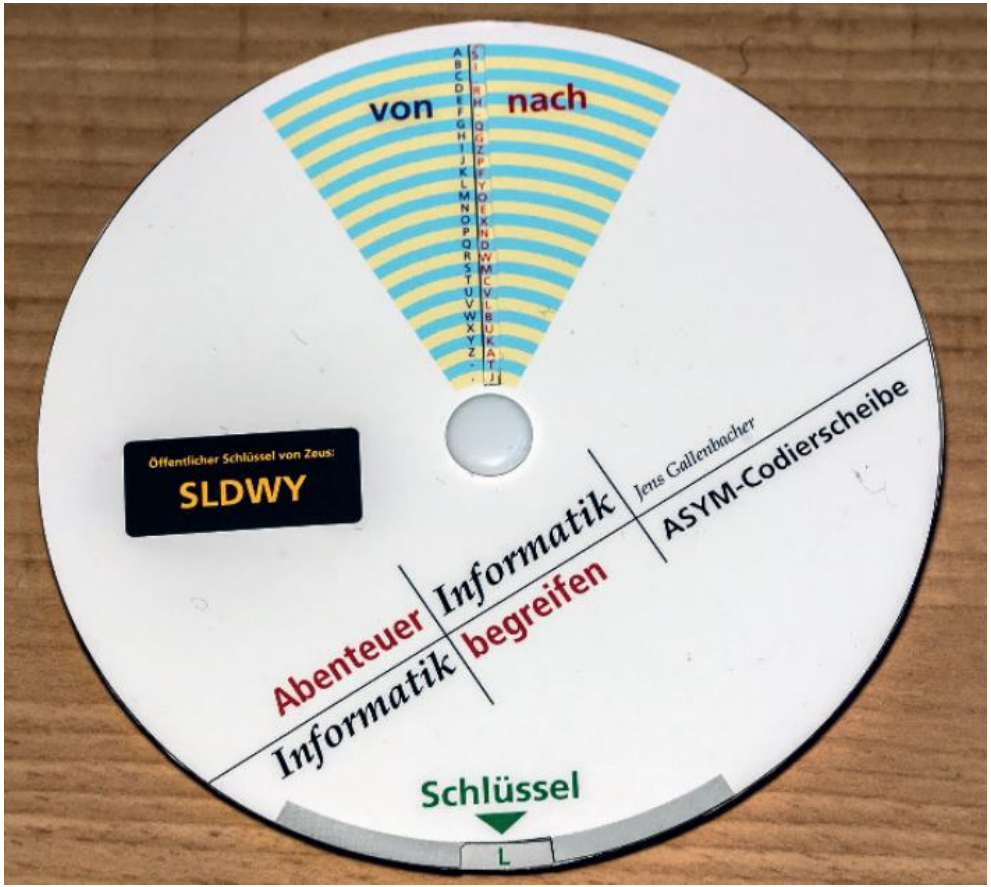


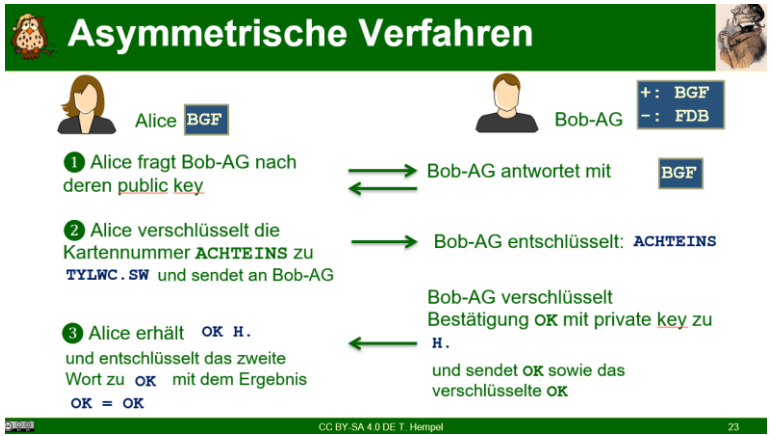
aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.

Asym. Verfahren

- das Prinzip der asymmetrischen Verschlüsselung erläutern

Aus Gallenbacher: Abenteuer Informatik. Kapitel 12. CC-BY-NC-ND 4.0

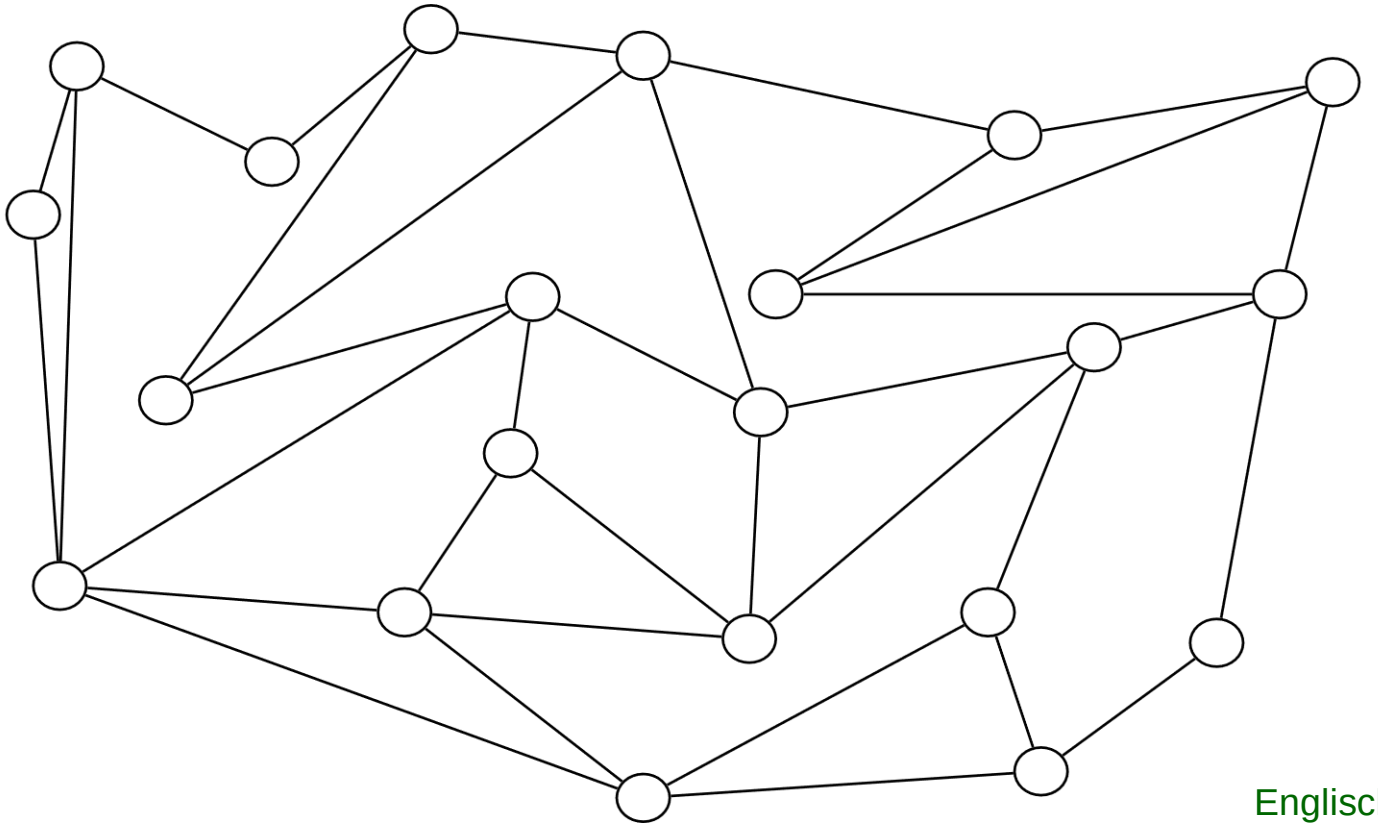




https://t1p.de/6j42

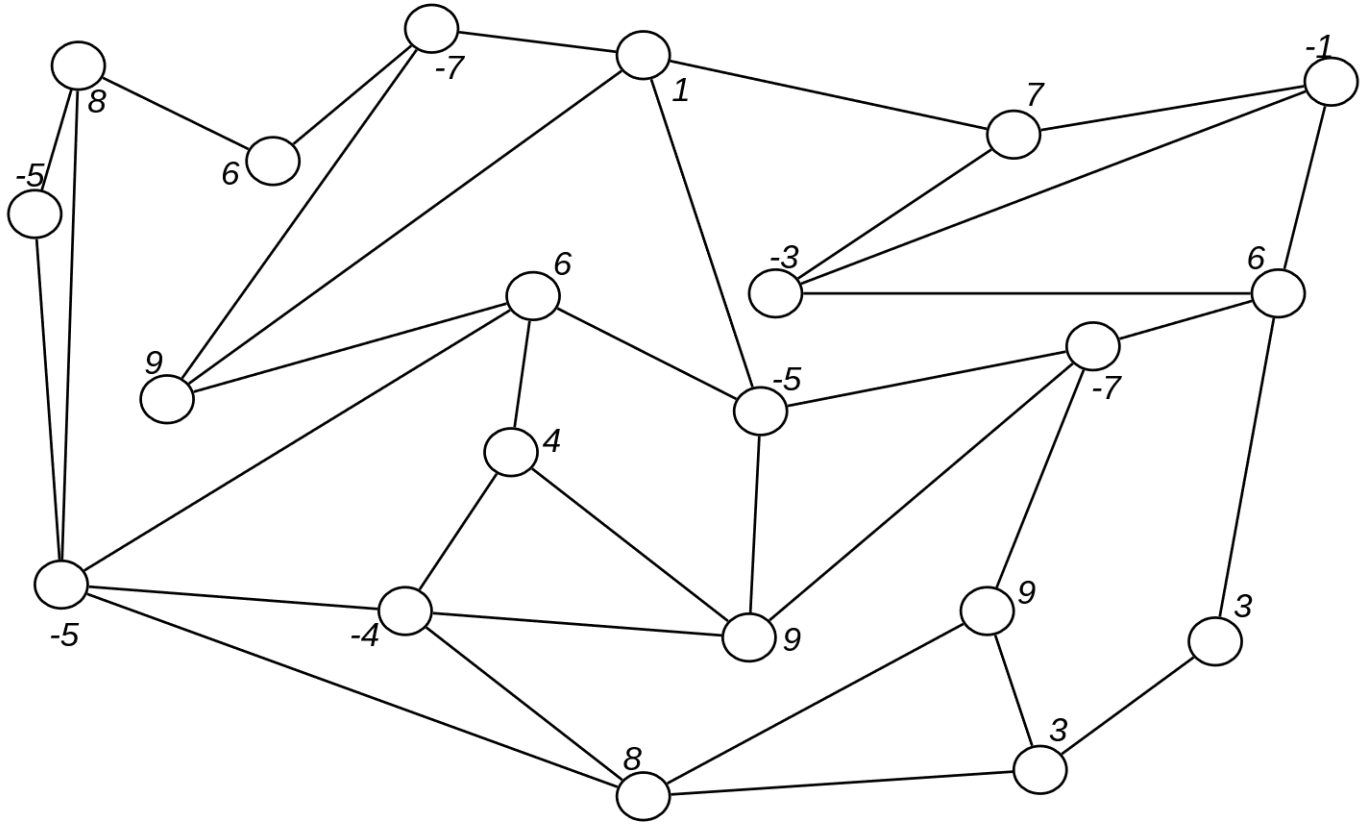
https://t1p.de/5cth

Kid Krypto



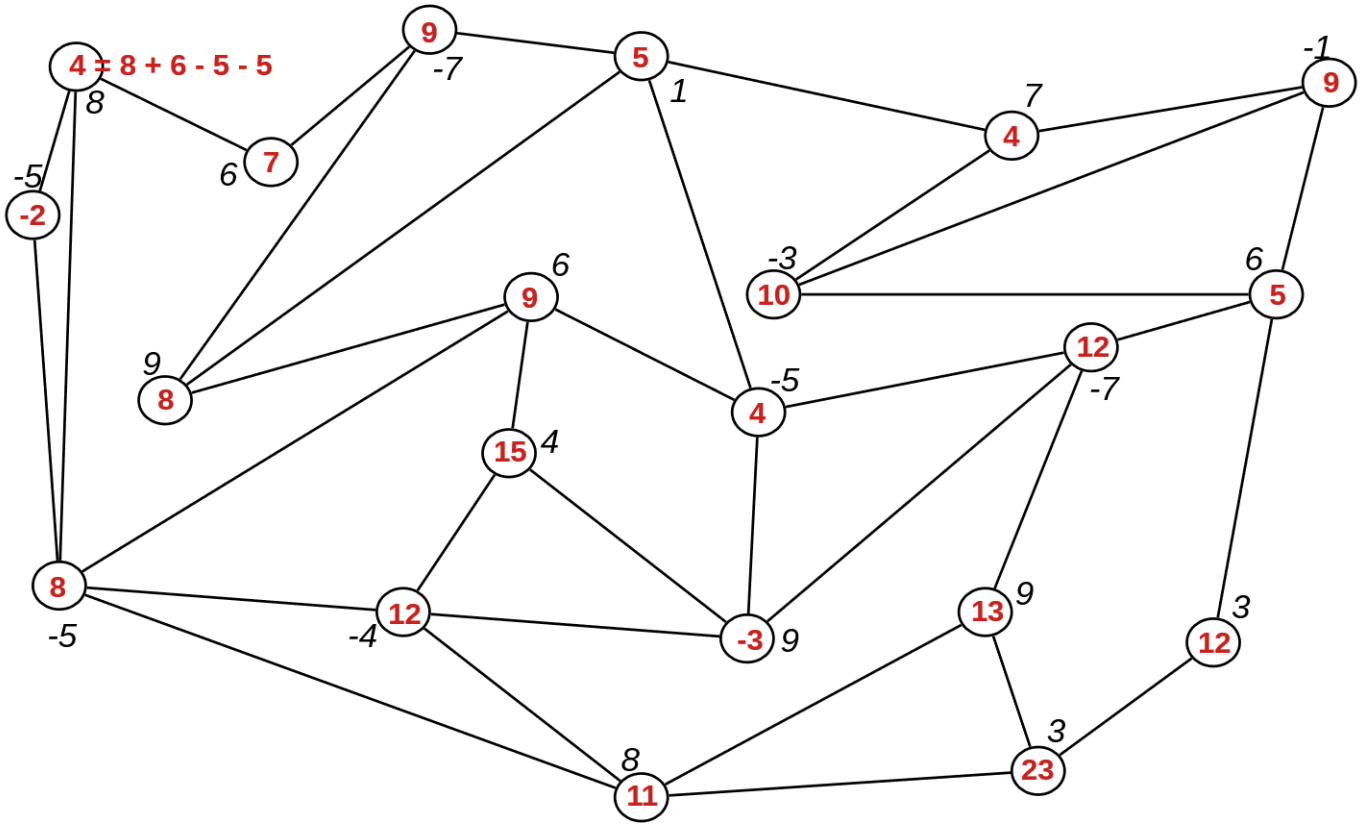
Englisch: https://t1p.de/9nh5
Deutsch: https://t1p.de/djz2

Kid Krypto

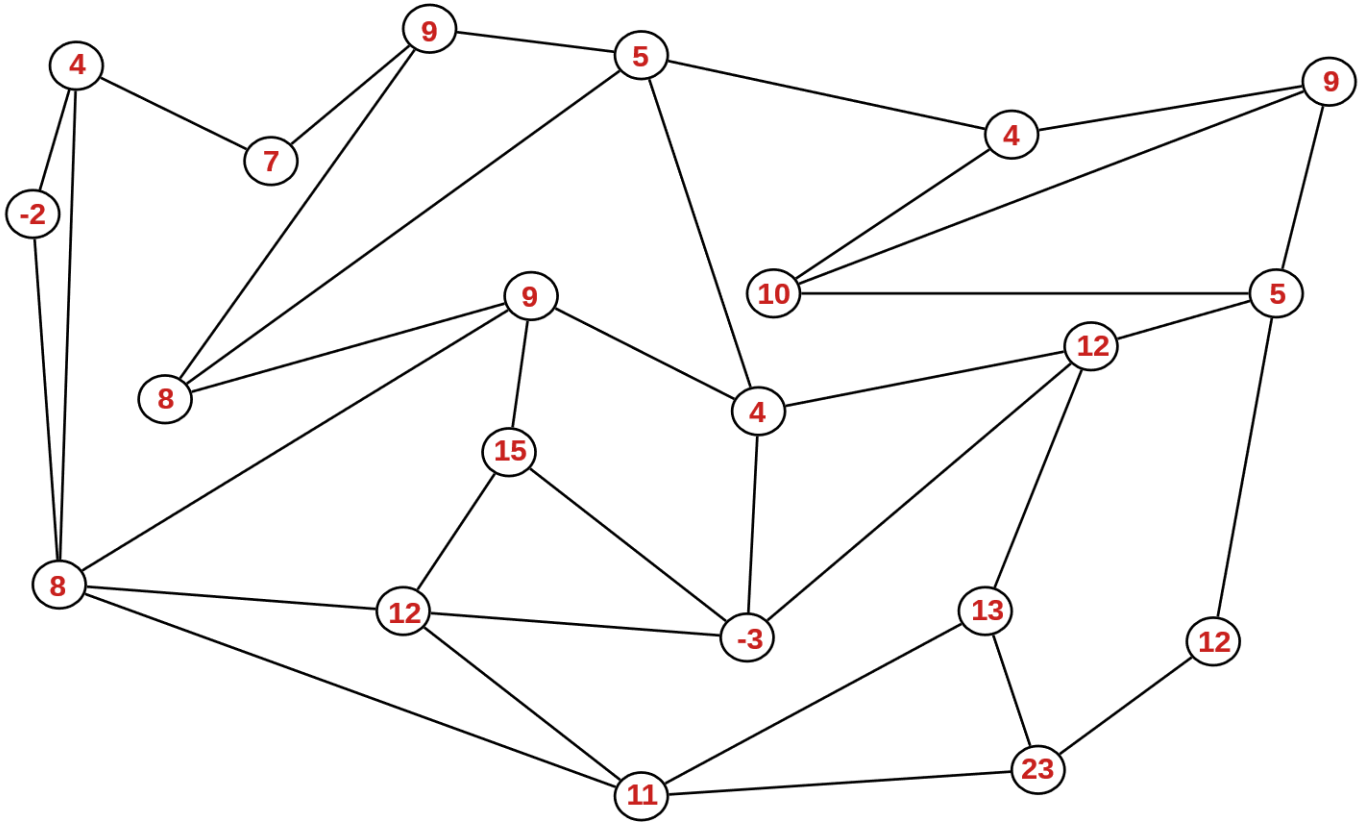


8
+6
-7
+1
+7
-1
-5
-3
+6
+9+6
-5
-7
-5
+4-4
+9
+9
+8
+3
+3
42

Kid Krypto



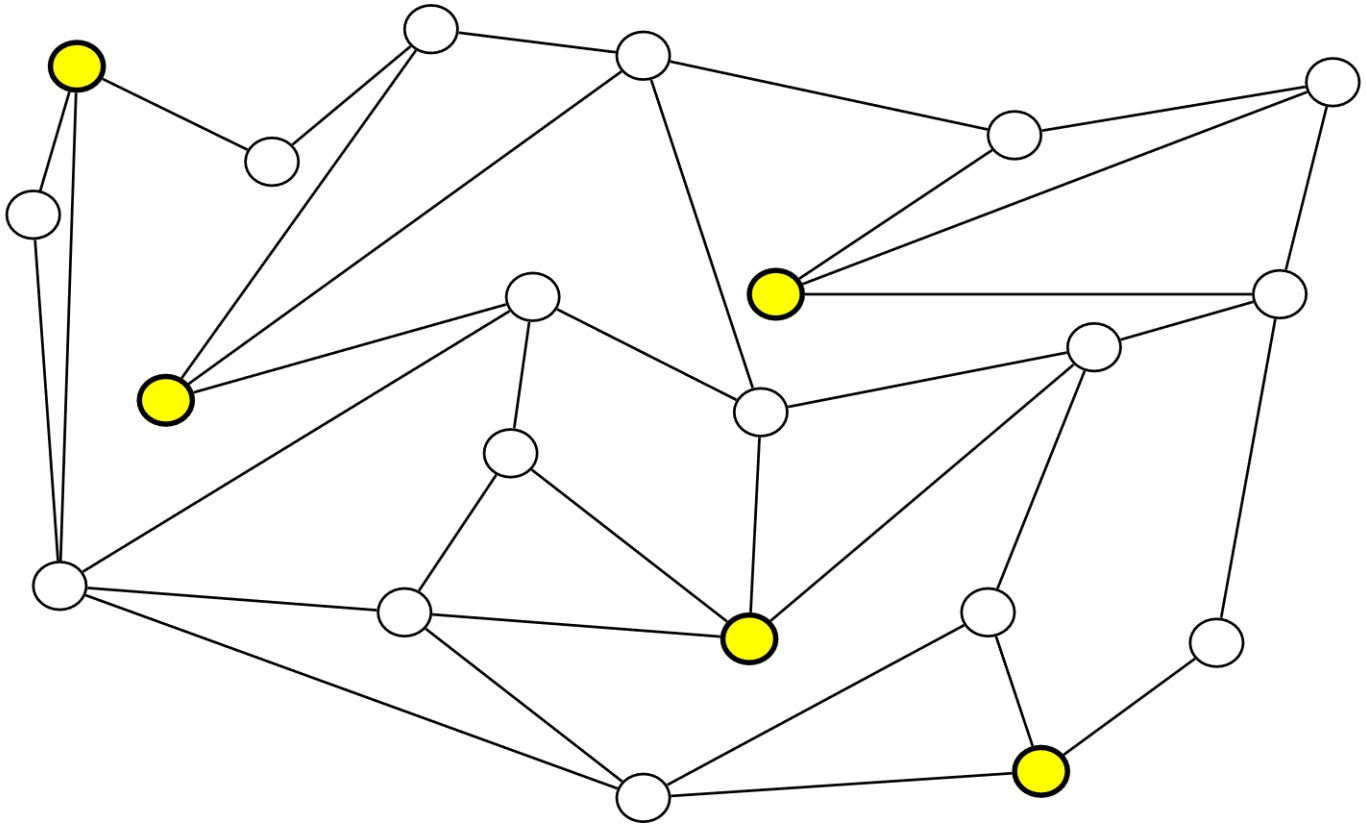
Kid Krypto



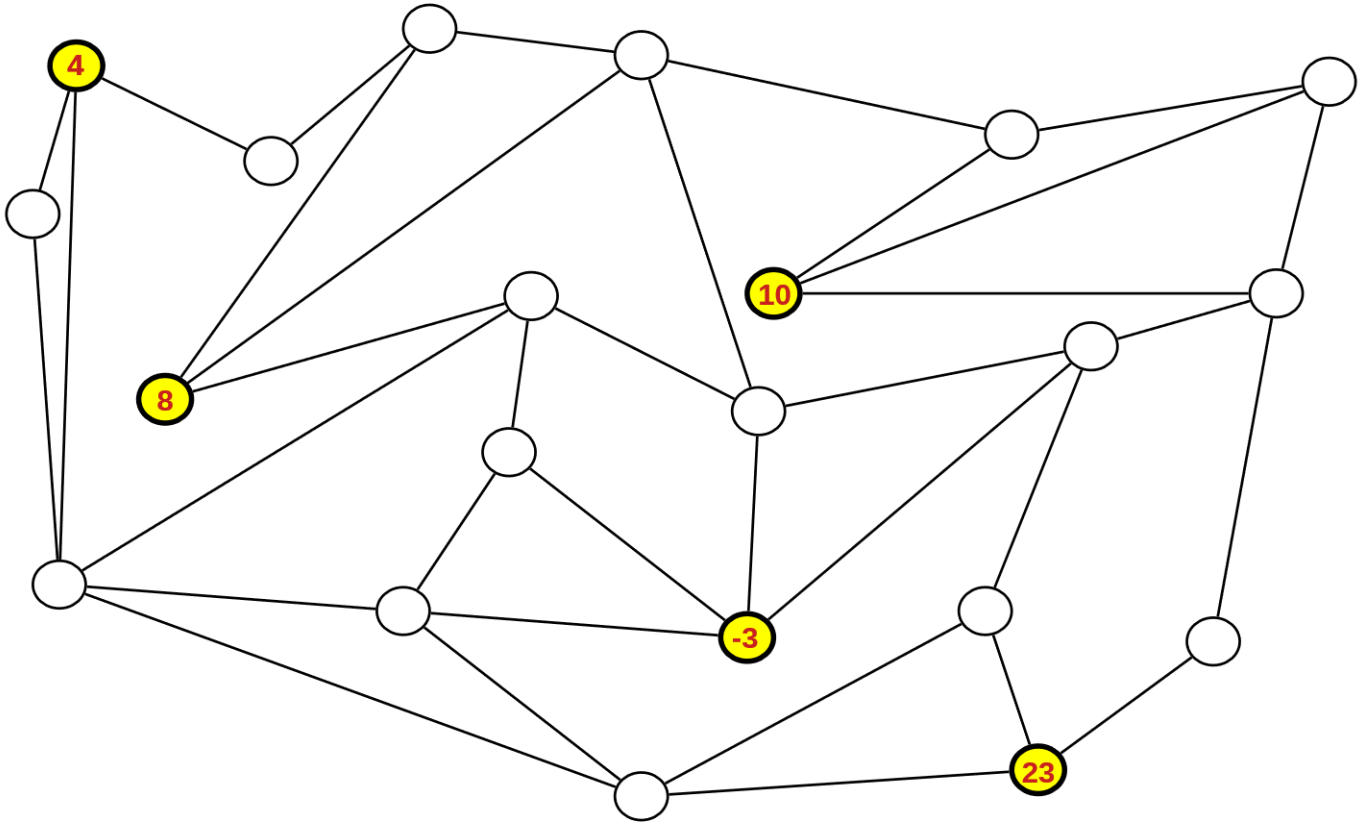
Einwegfunktionen

Das Prinzip der Einwegfunktion ist anschaulich darzustellen.

Kid Krypto

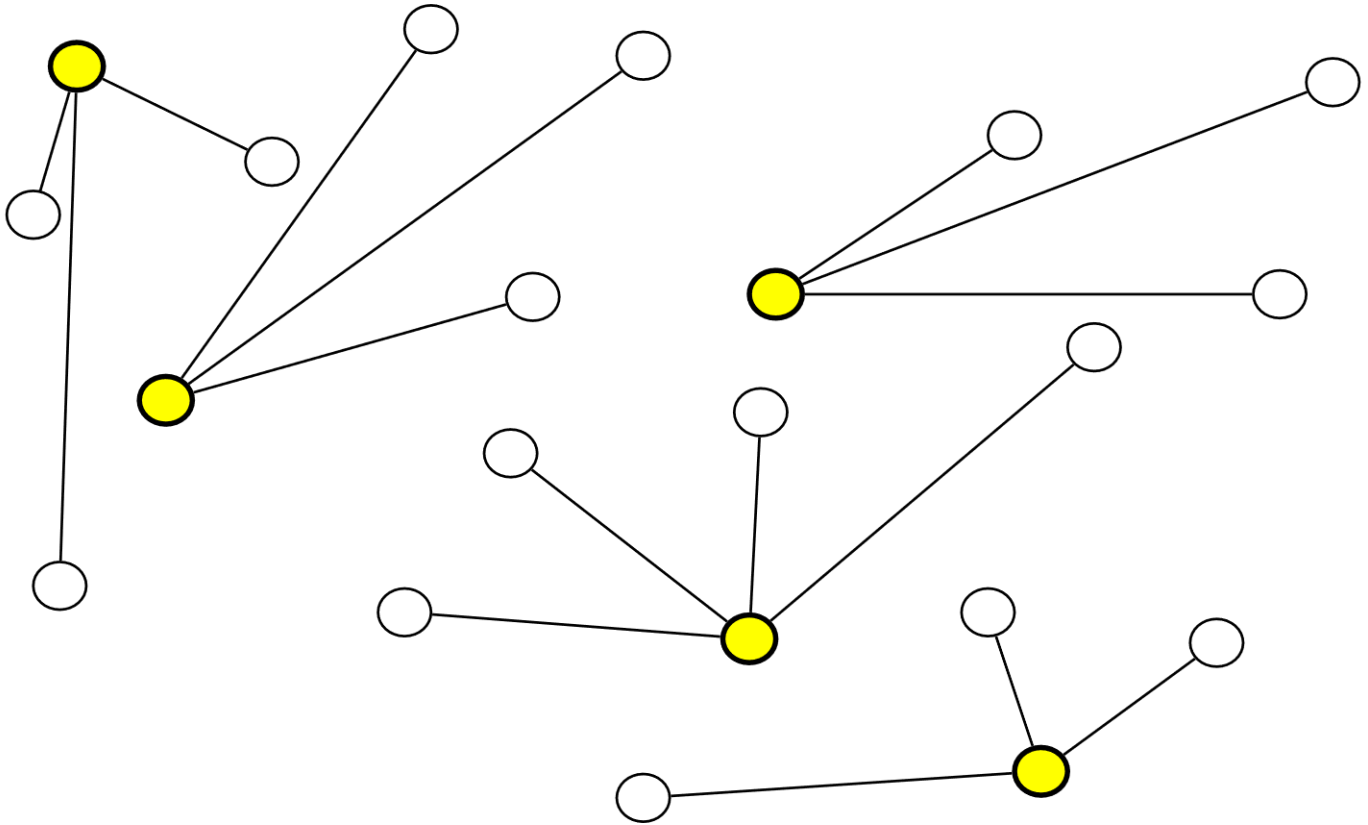


Kid Krypto




```
  4
+10
+ 8
- 3
+23
 42
```

Kid Krypto



Hashing

Das Prinzip der Einwegfunktion ist anschaulich darzustellen.

- das Prinzip der Einwegfunktion anhand einer Hashfunktion erläutern LK

```java
public class Konto {

  // Anfang Attribute
  private int nummer;
  private String art;
  private int saldo;
  private int hash;
  private boolean angemeldet;
  private Kunde inhaber;
  // Ende Attribute

  /**
   * Konstruktor für Objekte der Klasse Konto
   * @param pNummer Kontonummer
   * @param pSaldo Saldo
   * @param pArt Giro oder Spar
   * @param pInhaber
   */
  public Konto(int pNummer, int pSaldo, String pArt, Kunde pInhaber) {
    this.nummer = pNummer;
    this.saldo = pSaldo;
    this.art = pArt;
    this.inhaber = pInhaber;
    angemeldet = false;
    int pin = (int) ((9000) * Math.random() + 1000);
    System.out.println("Ihre PIN wurde generiert auf "+pin);
    this.hash = String.valueOf(pin).hashCode();
```

Hashing

Das Prinzip der Einwegfunktion ist anschaulich darzustellen.

- das Prinzip der Einwegfunktion anhand einer Hashfunktion erläutern LK

hashCode

```
public int hashCode()
```

Returns a hash code for this string. The hash code for a `String` object is computed as

```
s[0]*31^(n-1) + s[1]*31^(n-2) + ... + s[n-1]
```

using `int` arithmetic, where `s[i]` is the *i*th character of the string, `n` is the length of the string, and `^` indicates exponentiation. (The hash value of the empty string is zero.)

Overrides:

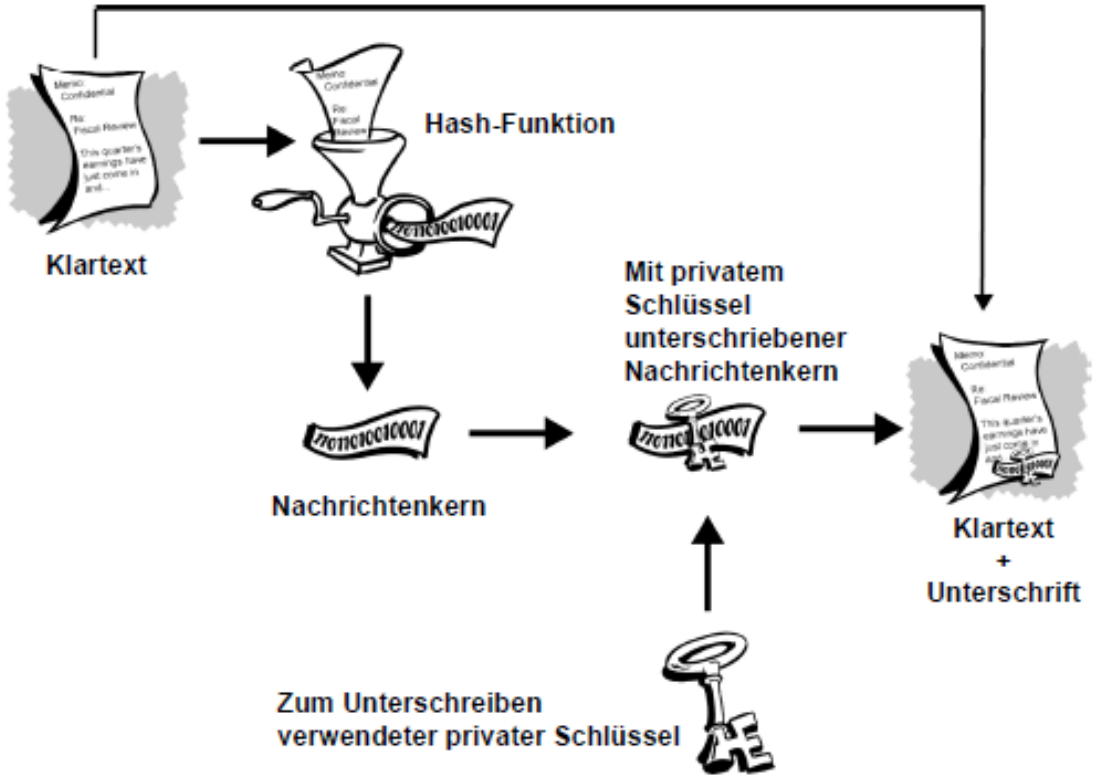
`hashCode` in class `Object`

Returns:

a hash code value for this object.

Digitale Signatur

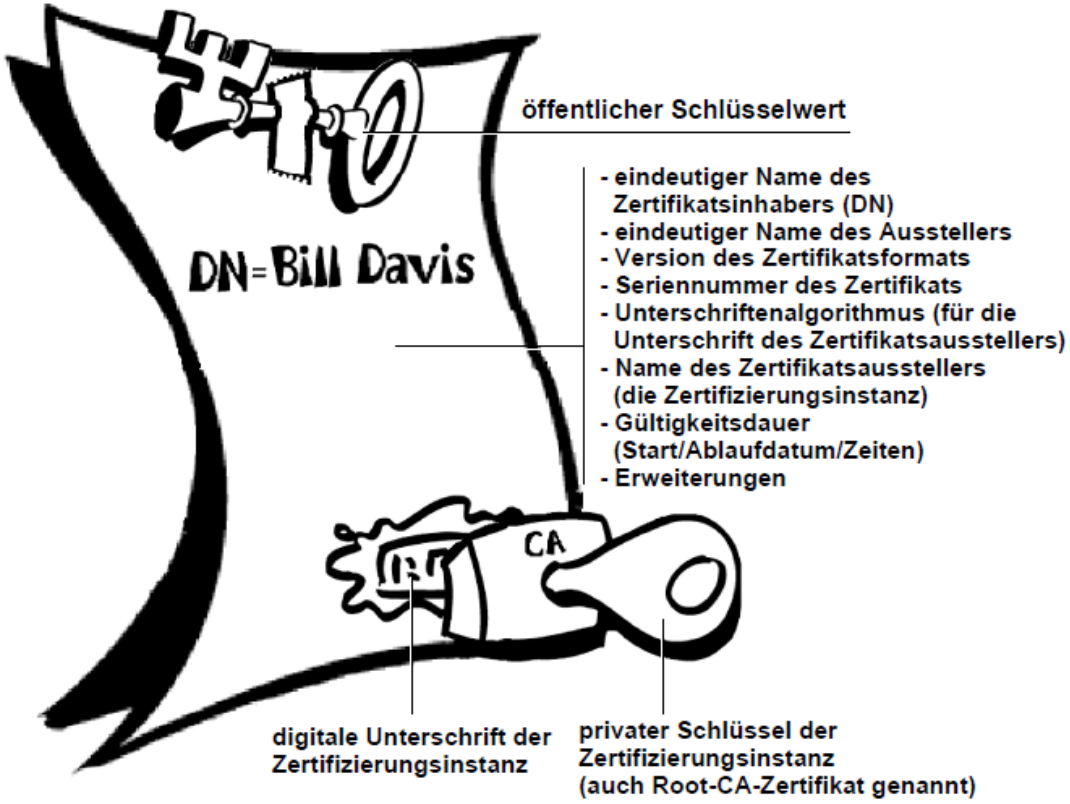
- die Prinzipien digital zertifizierter und signierter Daten erläutern



aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.

Zertifikate

- die Prinzipien digital zertifizierter und signierter Daten erläutern



aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.

Zertifikate

- die Prinzipien digital zertifizierter und signierter Daten erläutern

Alice **TC SLDWY**

+: CEF
-: ZLB
TC SLDWY

Trust Center

+: SLDWY
-: TEG-V
Bob-AG BGF
Mr. X CEF

❶ Alice verschlüsselt die Frage nach public key Bob-AG zu **LXMCHM** und fragt TC

→ TC entschlüsselt zu **BOB-AG** und antwortet mit der signierten Information

← **BOB-AG.BGF JMGKKFCGEH**

❷ Alice prüft die Signatur und erhält

BOB-AG.BGF BOB-AG.BGF

Verschlüsselung

LK
- das Prinzip der hybriden Verschlüsselung beschreiben und dessen Nutzen begründen

- z. B. Diffie-Hellman-Schlüsseltausch

Ein Pfund Gehacktes

Wissen macht Ah! | 03.01.2019 | 24:41 Min. | Verfügbar bis 03.01.2024 | KiKa

Grenzen

- die Grenzen der modernen Kryptografie anhand der Einwegfunktionen erläutern

Rainbow tables

Rainbow-tables sind riesige Sammlungen vorberechneter Hash Werte. Im Beispiel vorhin, haben wir Google als Rainbow-table missbraucht, um das dazugehörende Passwort zu finden. Genaugenommen müssten wir von "Lookup-tables" sprechen, Rainbow-tables sind komplexer, die Idee ist aber dieselbe.

Ein Beispiel einer Rainbow-table könnte etwa wie folgt aussehen:

Passwort	MD5-Hash
...	...
schatzinsel	39b7ed33ff1d275ac2dc8f772e86c757
schatzkarte	032e49ff68095f86258109269de15e39
schatztruhe	e4ca741a4dc2f86271be4fe7b13e65d3
...	...

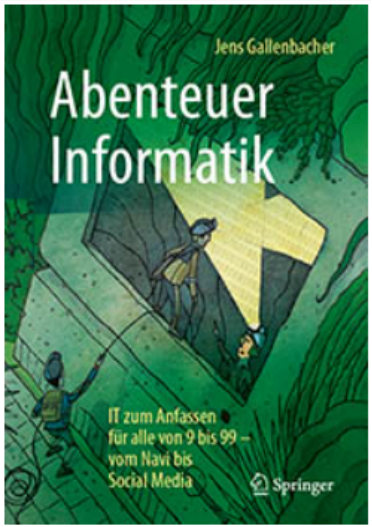
Stellen wir uns vor, wir erstellen eine Rainbow-table die alle Wörter aus einem deutschen Duden (≈150'000), alle Namen aus einem Telefonbuch (≈5'000'000), und alle Zeichenkombinationen bis zu 6 Stellen (19'770'609'664) enthält. Wir erhalten eine Tabelle mit **19'775'759'664** vorberechneten Hash Werten.

Heutzutage werden oft Grafikkarten (GPUs) zur Suche von Hashwerten eingesetzt, da diese extrem schnell parallele Berechnungen erledigen können. Eine handelsübliche GPU bewältigt bis zu ~50 Giga MD5 Werte pro Sekunde (Stand 2021), um unsere Beispiel Rainbow-table zu erstellen braucht man also nur **0.4 Sekunden!**

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Materialien



NEU: Etliche Kapitel seit November 2020 Open Access

Die Kapitel 1, 2, 3, 8, 9, 11, 12, 14 und 15 sind seit November 2020 unter der Lizenz CC-BY-NC-ND 4.0 für alle kostenlos zugänglich. Sie dürfen diesen Auszug als PDF herunterladen, ausdrucken und sogar weitergeben, solange Sie keine kommerziellen Ziele damit verfolgen und keine Veränderungen vornehmen.

Sie können hier mehrere Versionen laden:

Die **Leseversion** ist zum Anschauen und Lesen auf dem Bildschirm am besten geeignet. Die Empfehlung ist, das Programm auf Anzeige/Seitenansicht/Zweiseitenansicht zu stellen, da so die Ränder korrekt dargestellt werden.

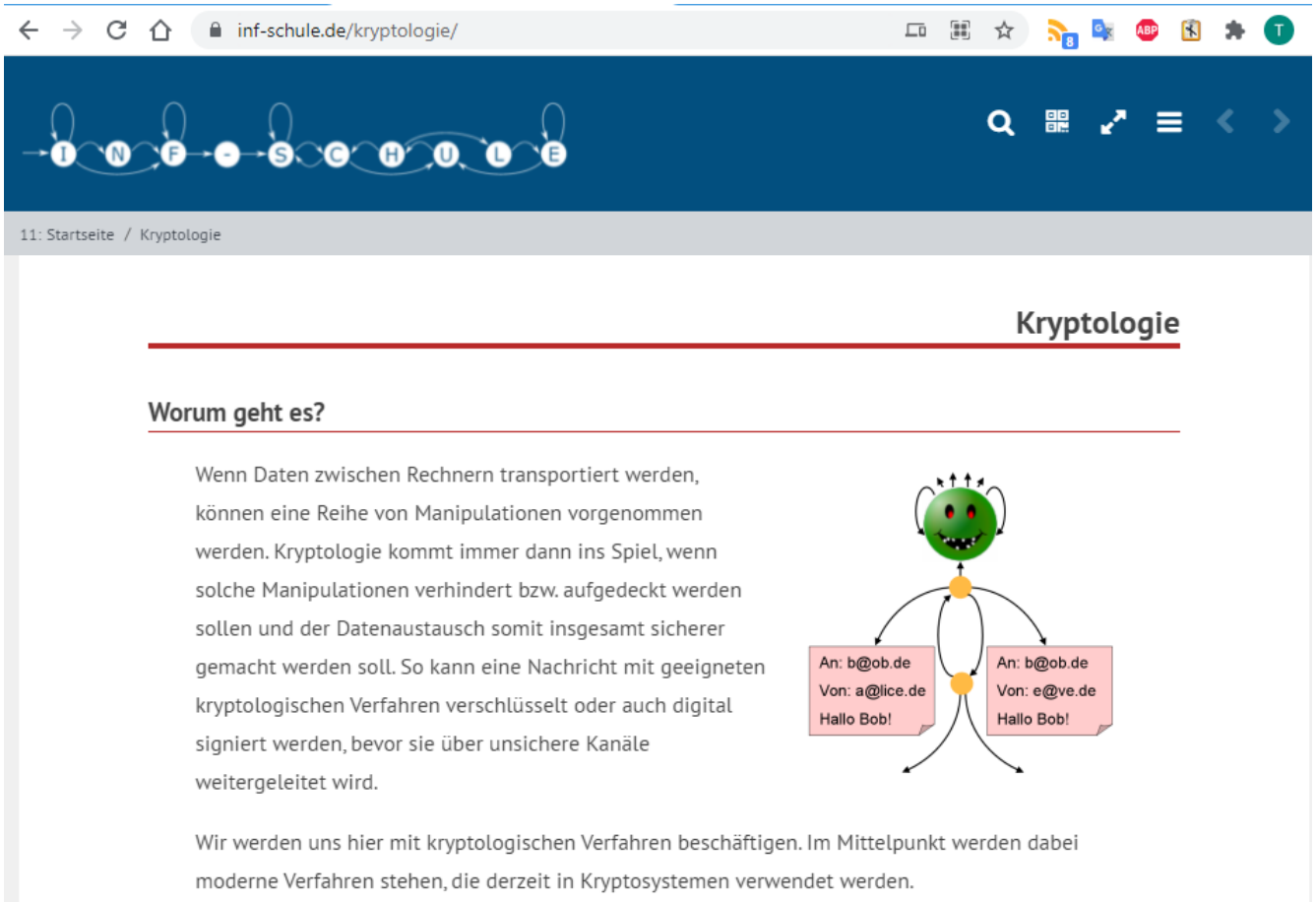
Die **Druckversion A4** ist zum Ausdrucken auf entsprechenden Druckern vorgesehen. Wenn Sie duplex (zweiseitig) drucken, sollten Sie "lange Seite" einstellen und können das Papier dann an einer Seite binden.

Die **Druckversion A3** ist zum Ausdrucken auf A3-Format vorgesehen und so "ausgeschossen", dass die Seitenzuordnung genau stimmt, wenn Sie die Blätter in der Mitte heften und falten. Dafür müssen Sie unbedingt duplex (zweiseitig) drucken und "kurze Seite" einstellen (!!!) Selbstverständlich können Sie die Version auch auf A4 drucken, um insgesamt ein A5-Heft zu erzeugen, das man aber nur noch mit sehr guten Augen lesen kann...

Alle Versionen sind der Konsistenz halber im Originalformat des Buches.

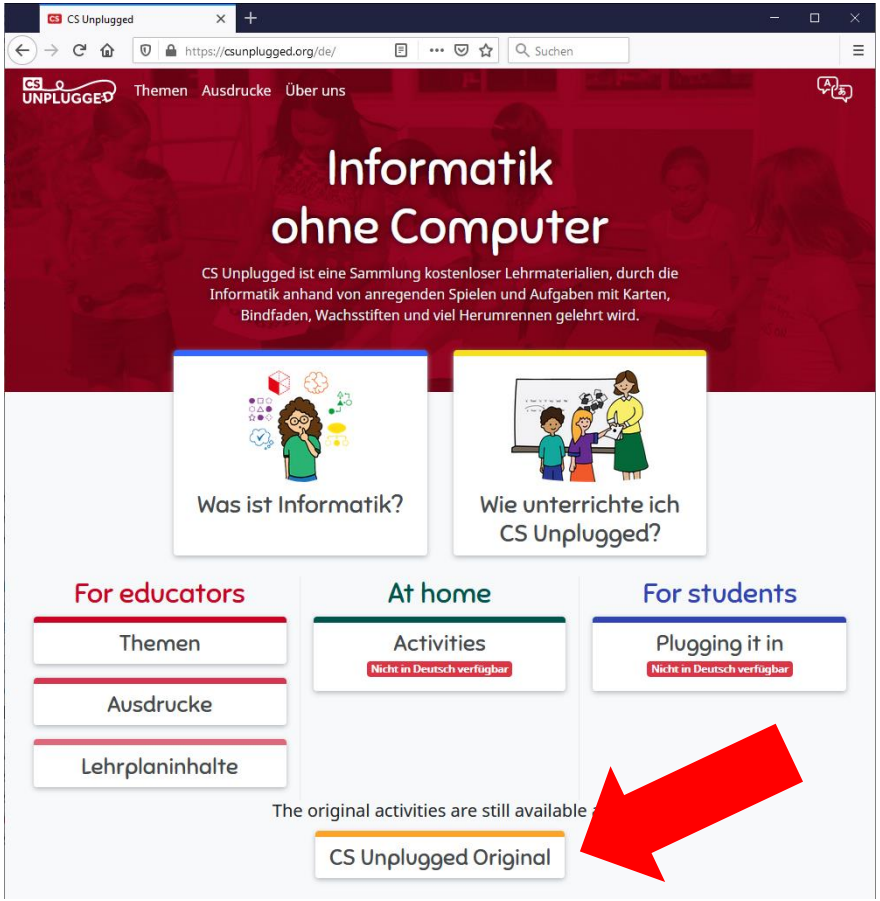
https://t1p.de/5cth

Materialien



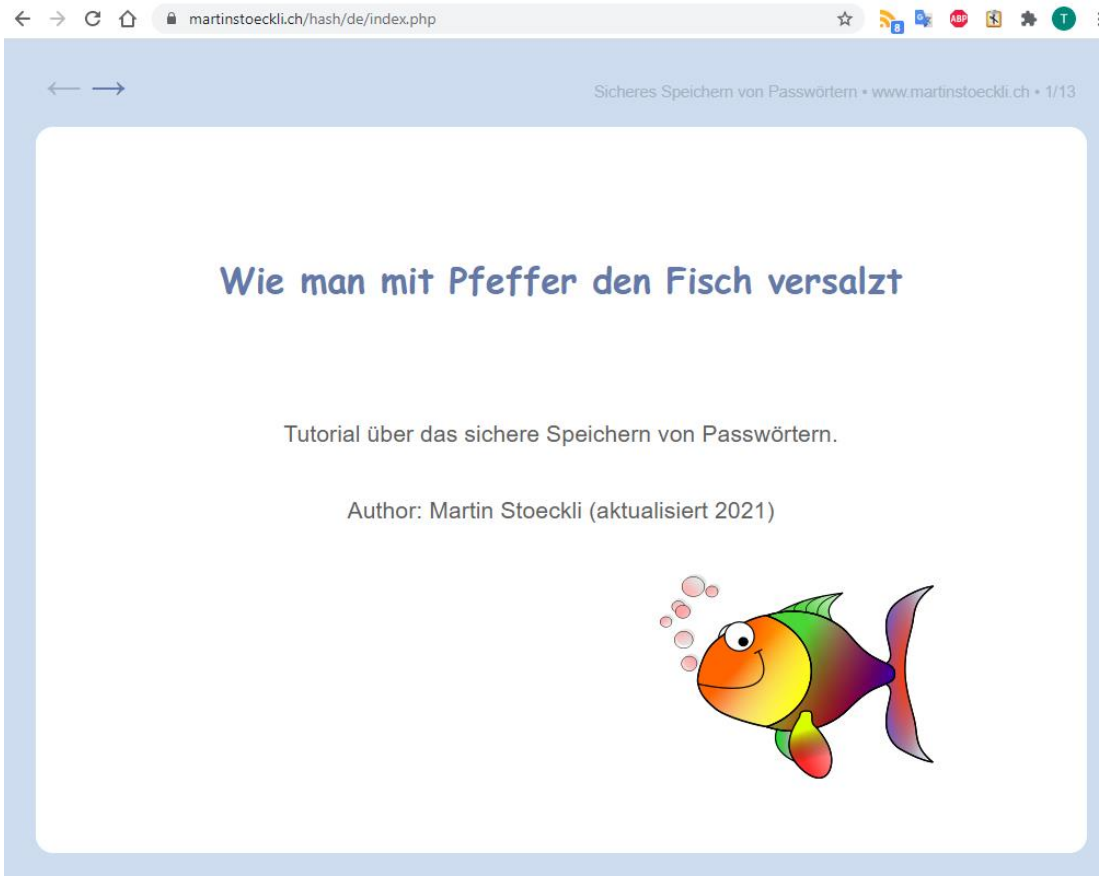
https://t1p.de/6mof

Materialien



https://t1p.de/kmea8

Materialien



https://t1p.de/h7de

Materialien

heise online heise+

IT Wissen Mobiles Security Developer Entertainment Netzpolitik W

TOPTHEMEN: WINDOWS 11 KRYPTOWÄHRUNGEN RAUMFAHRT APPLE PODCASTS

heise online ⟩ News ⟩ 10/2021 ⟩ Datenleck bei 3D-Druckplattform Thingiverse

Datenleck bei 3D-Druckplattform Thingiverse

Bereits seit einem Jahr soll eine Backupdatei mit Userdaten der Plattform Thingiverse in einem beliebten Hacker-Forum verfügbar sein.

Auch Passwörter betroffen

Passwörter seien nur verschlüsselt enthalten – allerdings *unsalted* und mittels der Algorithmen bcrypt und SHA-1 verschlüsselt, die als unsicher gelten. Gina Häußge, Maintainerin der 3D-Drucker-Software Octoprint3D, rät daher zum sofortigen Passworttausch und lieferte auf Twitter auch gleich eine Anleitung dazu.

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?

Aufgabentypen

Lernaufgaben	Prüfungsaufgaben
Alles außer Mathe	Autonom oder in Verknüpfung mit anderen Themengebieten: • Symmetrische Verfahren analysieren und beurteilen • Zur Sicherheit eines Verfahrens mithilfe des Kerckhoffsschen Prinzips argumentieren • Im Plan genannte Prinzipien und deren Einsatzmöglichkeiten erläutern

Fragen

- Wann bietet sich die Behandlung des Themas an?
- Was muss nicht vermittelt werden?
- Wie weit sind die fachlichen Grundlagen zu vermitteln?
- Wo gibt es Materialien?
- Welche Aufgaben kann man zum Thema stellen?
- …?