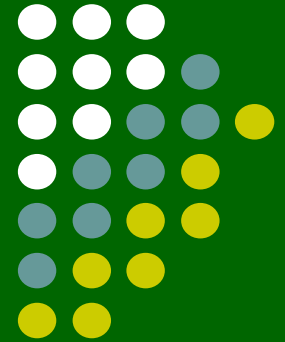


# 11/12.F2 Sichere Kommunikation





# Rahmenplan



Sichere Kommunikation [MD2] [MD4] [DRF]

ca. 9/14 Unterrichtsstunden

| Verbindliche Ziele und Inhalte                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Hinweise und Anregungen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Aspekte der Kryptologie</p> <ul style="list-style-type: none"><li>• Kommunikation mithilfe von Sequenzdiagrammen interpretieren und darstellen</li><li>• die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen</li><li>• die Sicherheit kryptografischer Verfahren mithilfe des Prinzips von Kerckhoffs prüfen</li><li>• das Prinzip der asymmetrischen Verschlüsselung erläutern</li><li>• die Prinzipien digital zertifizierter und signierter Daten erläutern</li><li>• die Grenzen der modernen Kryptografie anhand der Einwegfunktionen erläutern [MD6]</li></ul> | <p>Die Behandlung des Themas erfolgt anschaulich und ohne umfangreiche mathematische Berechnungen. Dazu können mono- und polyalphabetische Verschlüsselungsverfahren analysiert werden.</p> <p>Das One-Time-Pad ist als einzig sicheres Verfahren zu thematisieren.<br/>Das Prinzip der Einwegfunktion ist anschaulich darzustellen.</p> <p>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.</p> |



# 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

### Verbindliche Ziele und Inhalte

Klasse 9

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

RSA-Demo

RSA mit privatem und öffentlichem Schlüssel -- oder nur mit öffentlichem Schlüssel

- ☒ Wählen Sie zwei Primzahlen p und q. Die Zahl  $N = pq$  ist der öffentliche RSA-Modul, und  $\phi(N) = (p-1)(q-1)$  ist die Eulersche Phi-Funktion. Der öffentliche Schlüssel e ist teilerfremd zu  $\phi(N)$ . Daraus wird der geheime Schlüssel  $d = e^{-1} \pmod{\phi(N)}$  berechnet.
- ☐ Zur Verschlüsselung von Daten oder zur Verifikation einer Signatur genügt es, dass Sie die öffentlichen RSA-Parameter angeben: den RSA-Modul N und den öffentlichen Schlüssel e.

Primzahleingabe

Primzahl p

Primzahl q

Primzahlen generieren...

RSA-Parameter

RSA-Modul N

$\phi(N) = (p-1)(q-1)$

Öffentlicher Schlüssel e

Geheimer Schlüssel d

Parametrisieren

RSA-Verschlüsselung / Entschlüsselung mit d [Alphabet: 256]

Eingabe als ☒ Zahlen ☐ Zeichen für Alphabetisches System...

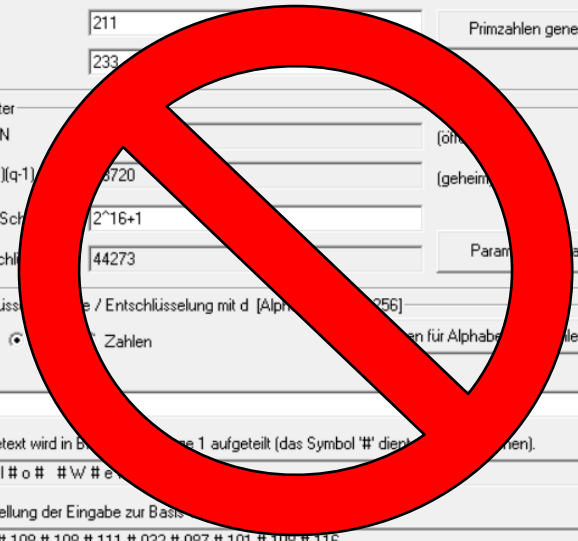
Eingabetext

Der Eingabetext wird in Blöcke der Größe 1 aufgeteilt (das Symbol '#' dient als Trennzeichen).

Zahlendarstellung der Eingabe zur Basis 256

Verschlüsselung in den Geheimtext  $c[i] = m[i]^e \pmod{N}$

Verschlüsseln Entschlüsseln Schließen





# 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?

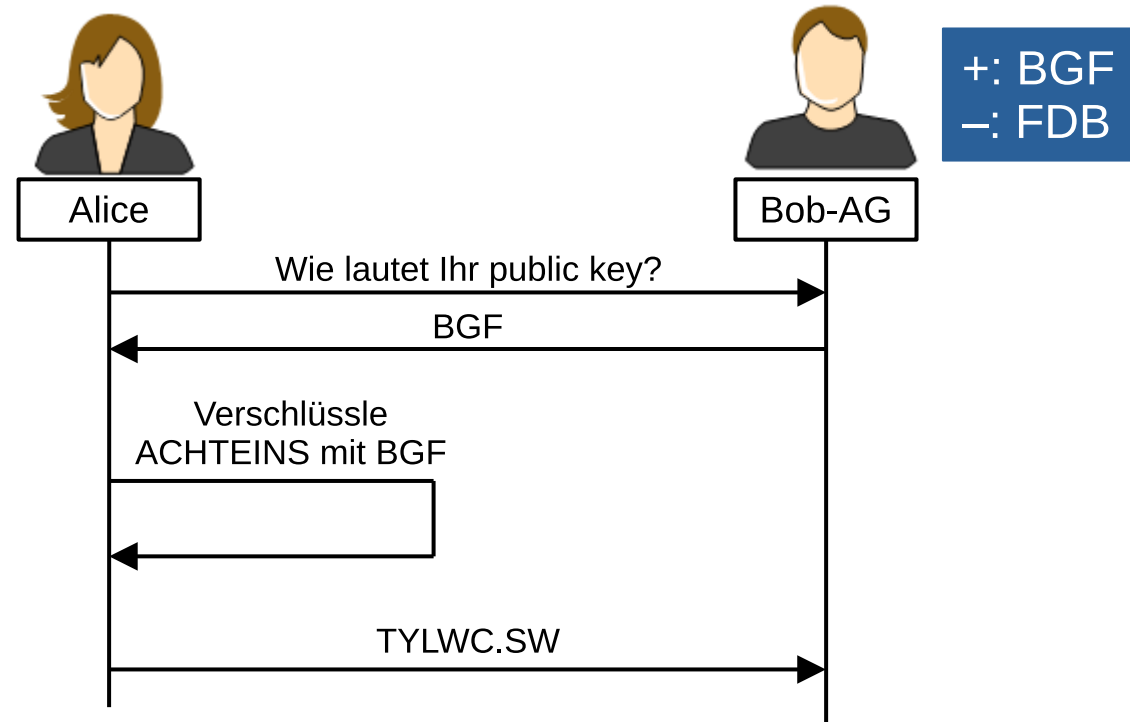


# Sequenzdiagramm

Kommunikation mithilfe von Sequenzdiagrammen interpretieren und darstellen



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





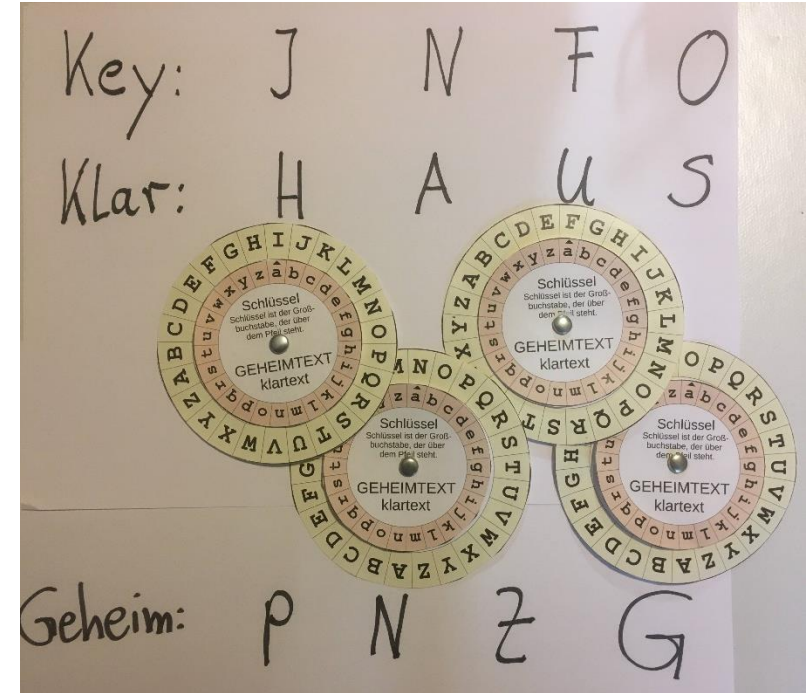
# Anschaulichkeit

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



## Ein Pfund Gehacktes

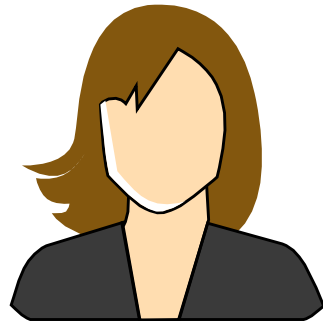
Wissen macht Ah! | 03.01.2019 | 24:41 Min. | Verfügbar bis 03.01.2024 | KiKa



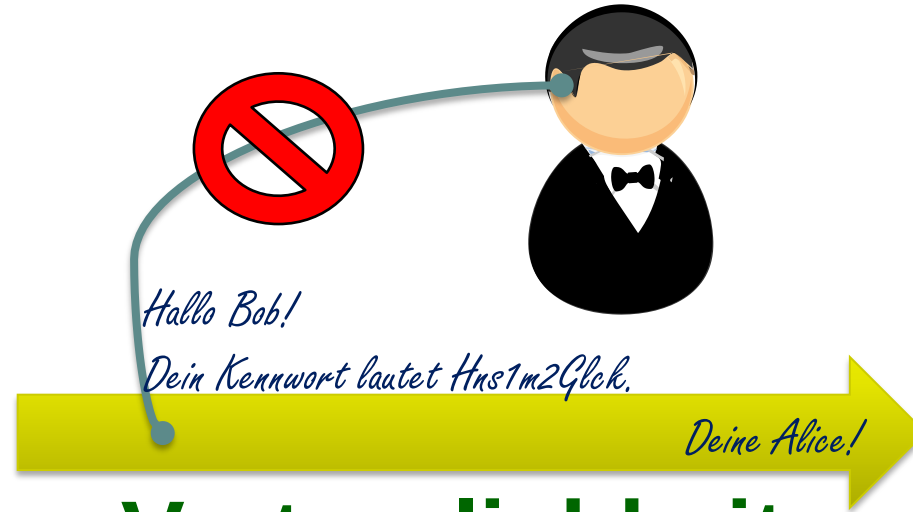


# Sicherheitsziele

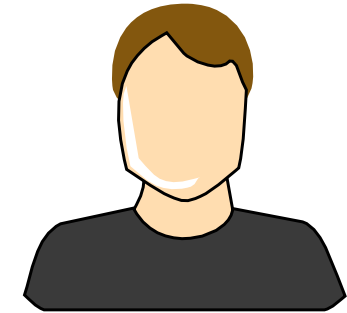
- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen



Alice



**Vertraulichkeit**  
kein Mitlesen durch Fremde



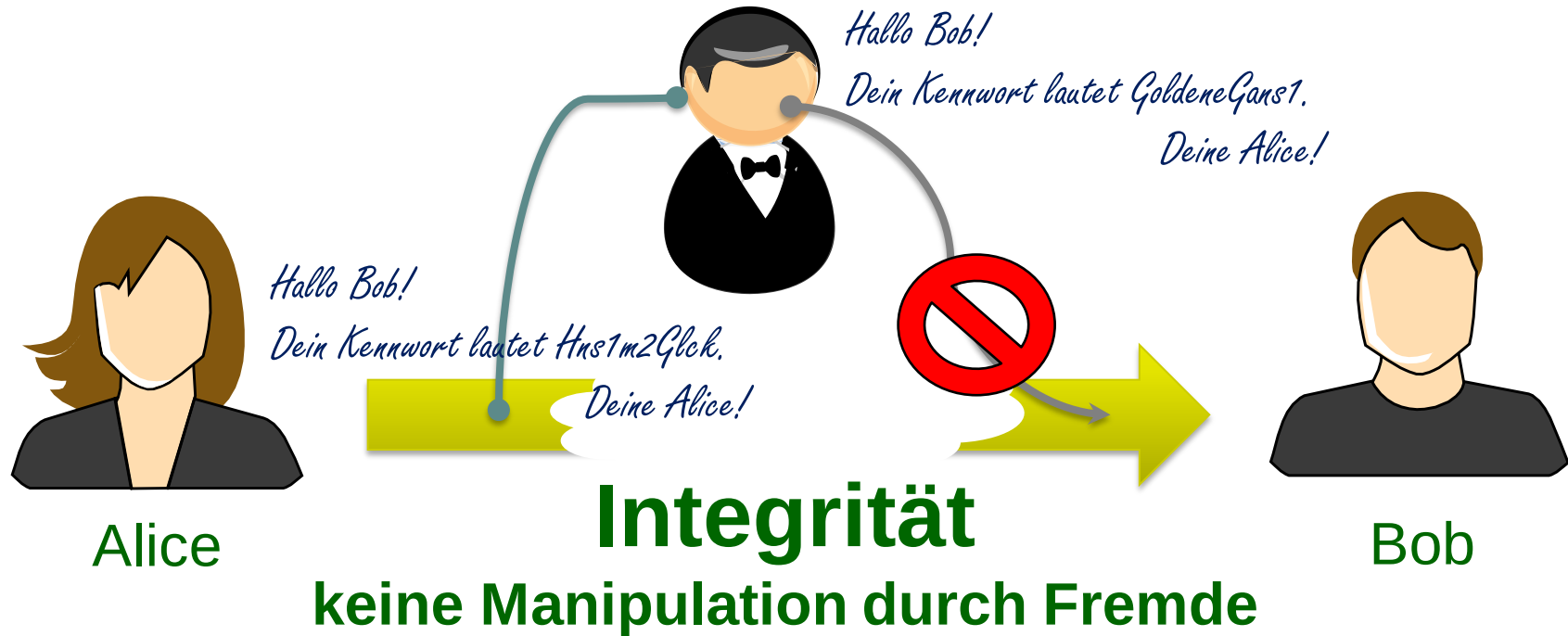
Bob

**Verschlüsselung**



# Sicherheitsziele

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



**Prüfziffern/Hash/Zertifikat**



# Sicherheitsziele

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



Alice

## Authentizität

Nachricht ist definitiv vom  
Absender

Bob

## Digitale Unterschrift



# Sicherheitsziele

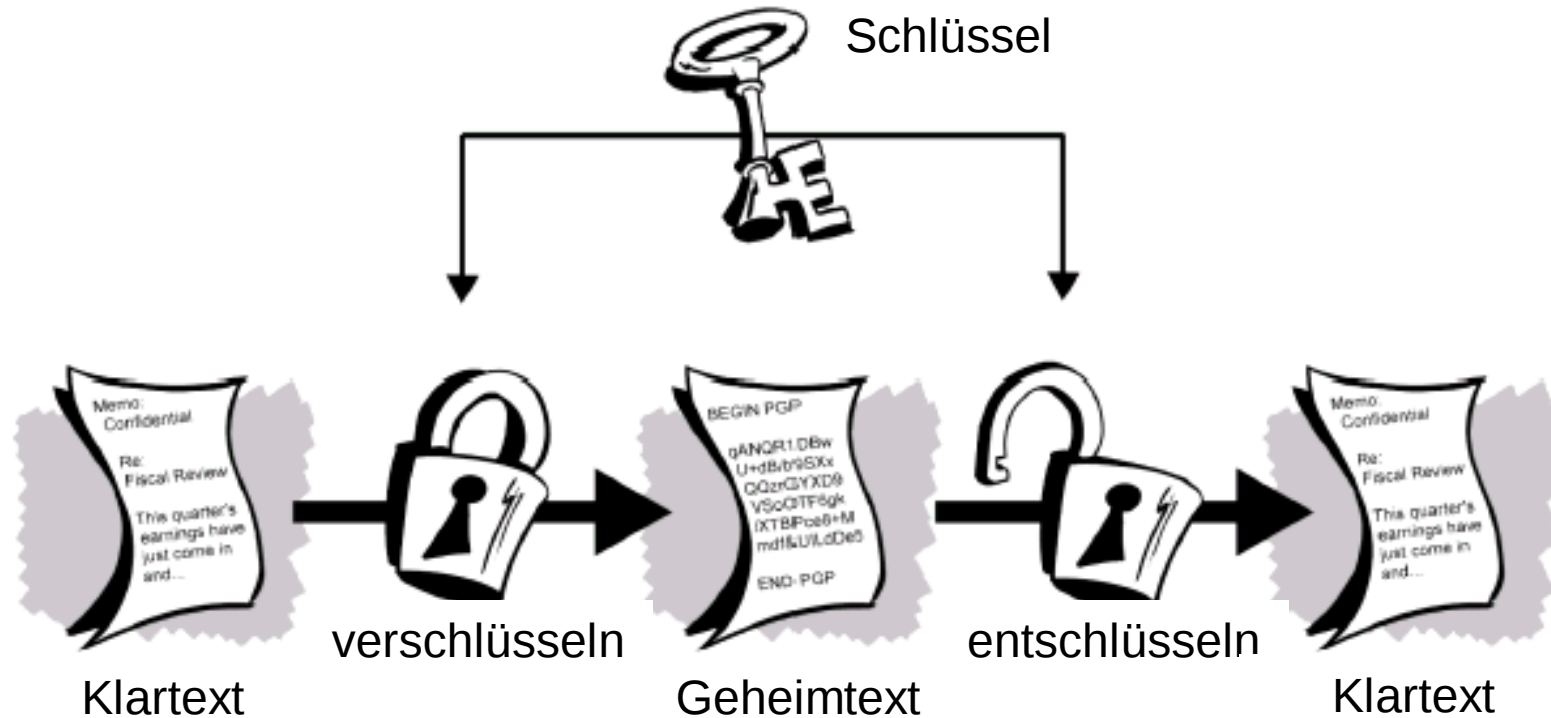
- die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit erläutern und begründen





# 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 polyalphabetische Verschlüsselungsverfahren analysiert werden.



## Steganographie verstecken

### Verborgene Schrift

Liebe Maria,  
das Wetter hier ist sehr schön,  
und dem Hund geht es auch schon  
viel besser. Hoffentlich ist bei dir  
alles in Ordnung.  
Pass auf dich auf, Joseph.  
Komm heute Nacht zum Ahornbaum

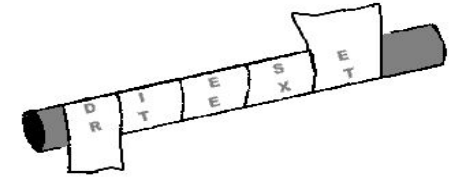


Nachrichten in unsichtbarer Tinte werden  
sichtbar, wenn sie von hinten erhitzt werden.  
Die Sicherheit hängt von absoluter  
Diskretion ab.  
Einfach zu entschlüsseln.

## Kryptografie verschlüsseln

### Substitution Zeichen/Wörter ersetzen

### Transposition Zeichen/Wörter umsortieren



### Monoalphabetisch Sherlock Holmes, Caesar



### Polyalphabetisch Vigenère, Enigma



### One Time Pad





# Vigenère-Verfahren

Dazu können mono- und polyalphabetische Verschlüsselungsverfahren analysiert werden.



Vigenère-Demonstration

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |

☒ Felder sperren

Verschlüsseln Entschlüsseln

Schlüssel  
GHEIM

Klartext  
WIRTSCHAFTSUNTERNEHMEN

Chiffre  
CMYXZQL

Buchstaben verschlüsseln

☐ Sonderzeichen ignorieren

☐ Blinken

☐ Animation

Rücksetzen

Umlaute Leerzeichen

Kleinschrift Großschrift

Schließen

- polyalphabetisches Verfahren
- symmetrisches Verfahren
- Tool zur Erarbeitung: Krypto



# One-Time-Pad

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



Vigenère-Demonstration

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |

☒ Felder sperren

Verschlüsseln Entschlüsseln

Schlüssel

UHTSMELURNCLSPCKDOEDI

Klartext

WIRTREFFENUNSUMVIERUHR

Chiffre

QPKLDIQZVAWYKJQ

Buchstaben verschlüsseln

☐ Sonderzeichen ignorieren

☐ Blinken

☐ Animation

Rücksetzen

Umlaute Leerzeichen

Kleinschrift Großschrift

Schließen

Schlüssel

UHTSMELURNCLSPCKDOEDI

Klartext

WIRTREFFENUNSUMVIERUHR

Chiffre

QPKLDIQZVAWYKJQ

- 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.



# Kerckhoffs 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.

- 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.

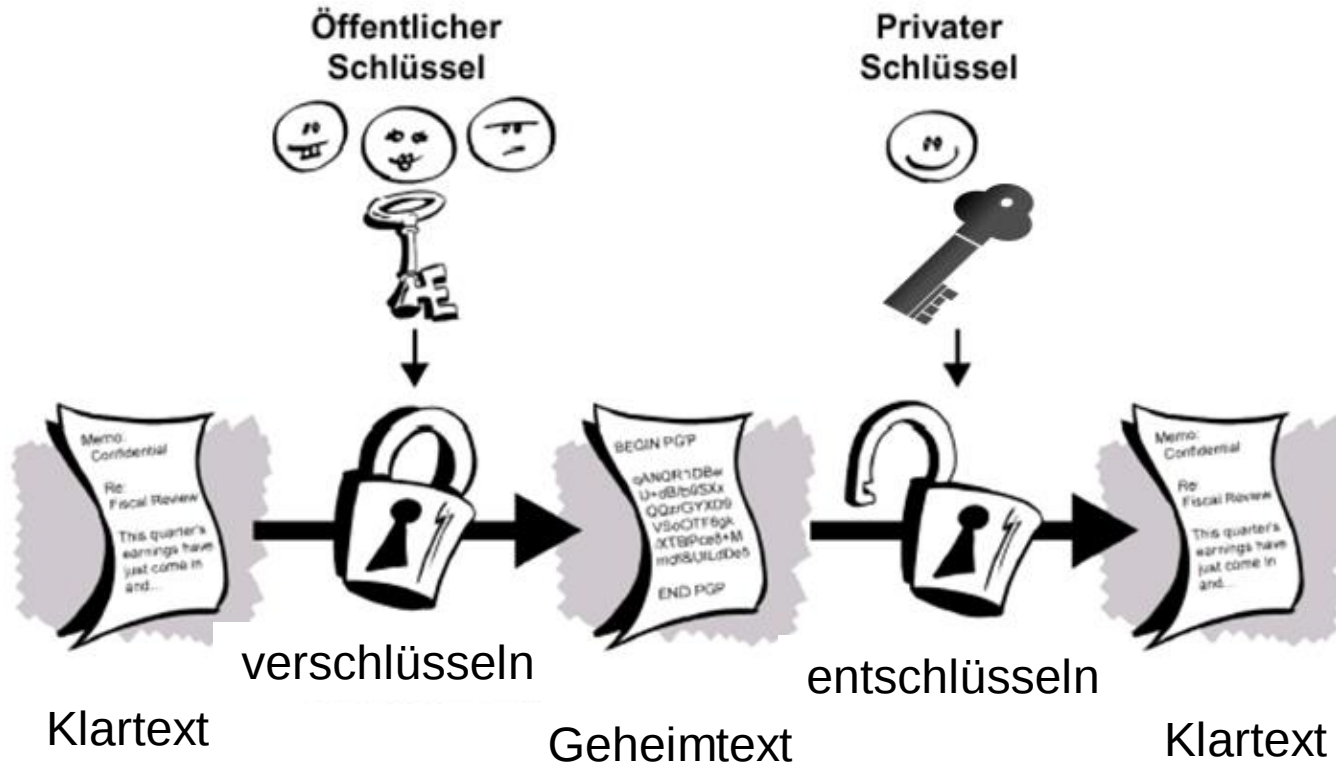


Eugen Drezen, Historio de la Mondo Lingvo (Leipzig, 1931), 102



# Asym. Verfahren

- das Prinzip der asymmetrischen Verschlüsselung erläutern

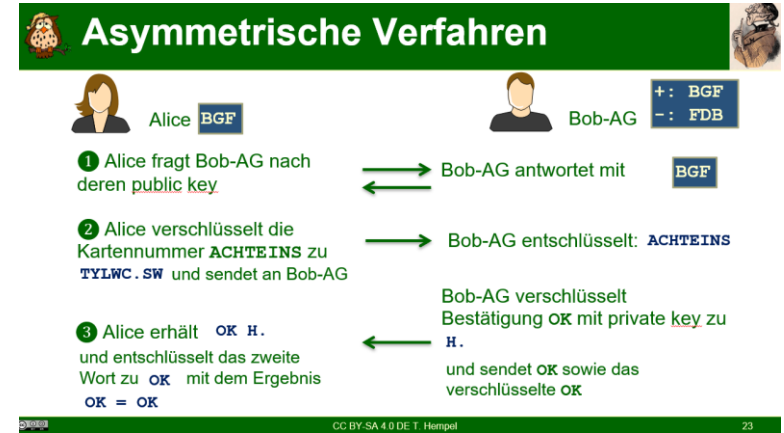


aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.



# Asym. Verfahren

- das Prinzip der asymmetrischen Verschlüsselung erläutern

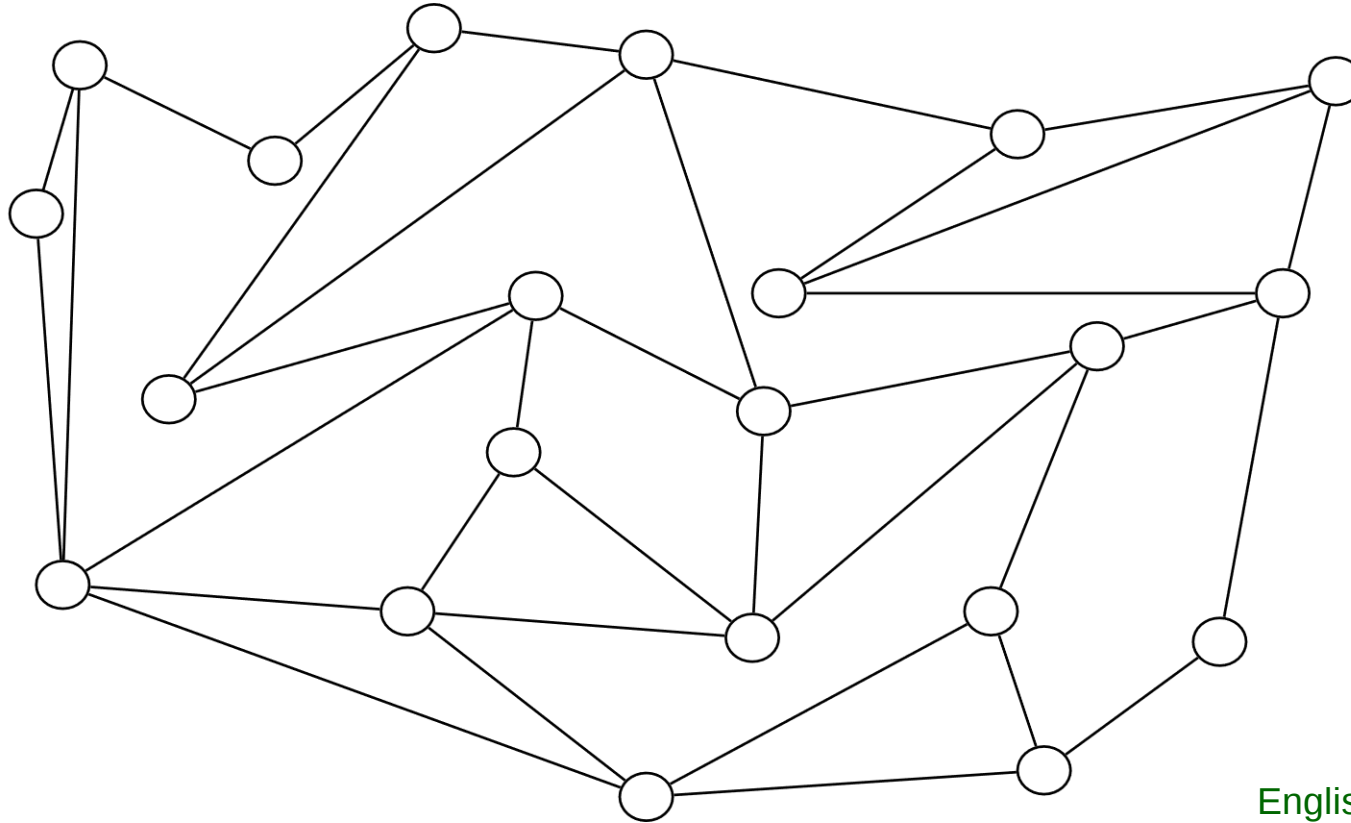


<https://t1p.de/6j42>

<https://t1p.de/5cth>



# Kid Krypto

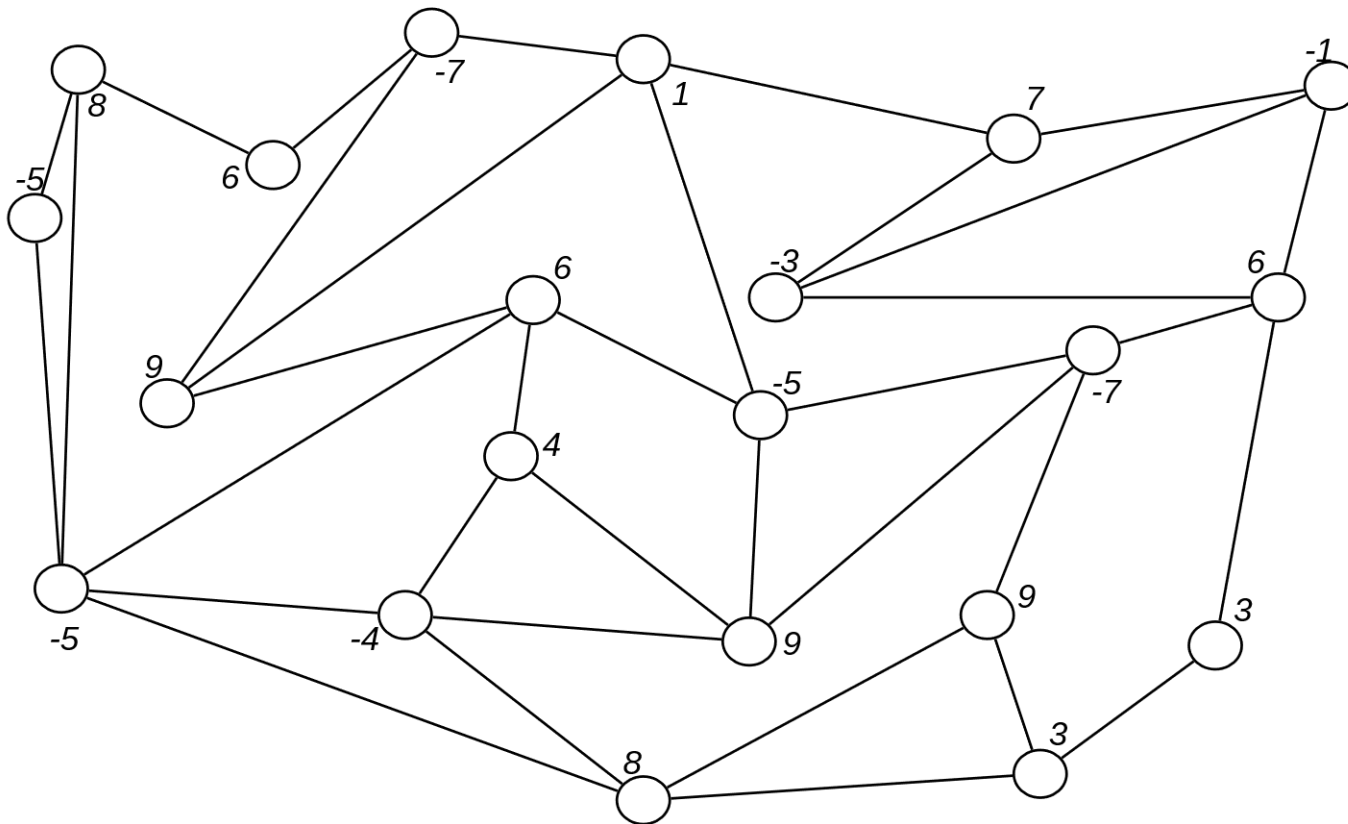


Englisch: <https://t1p.de/9nh5>

Deutsch: <https://t1p.de/djz2>



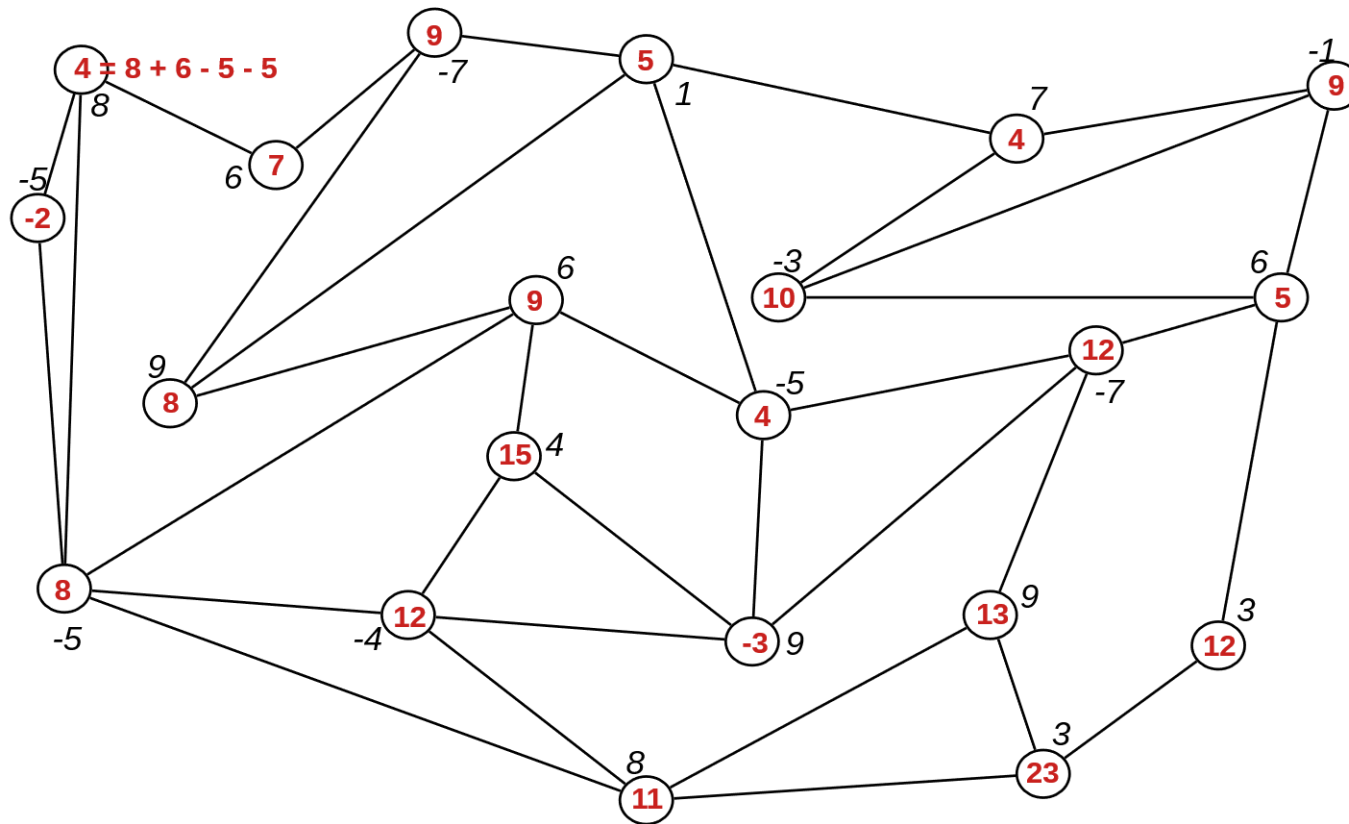
# Kid Krypto



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

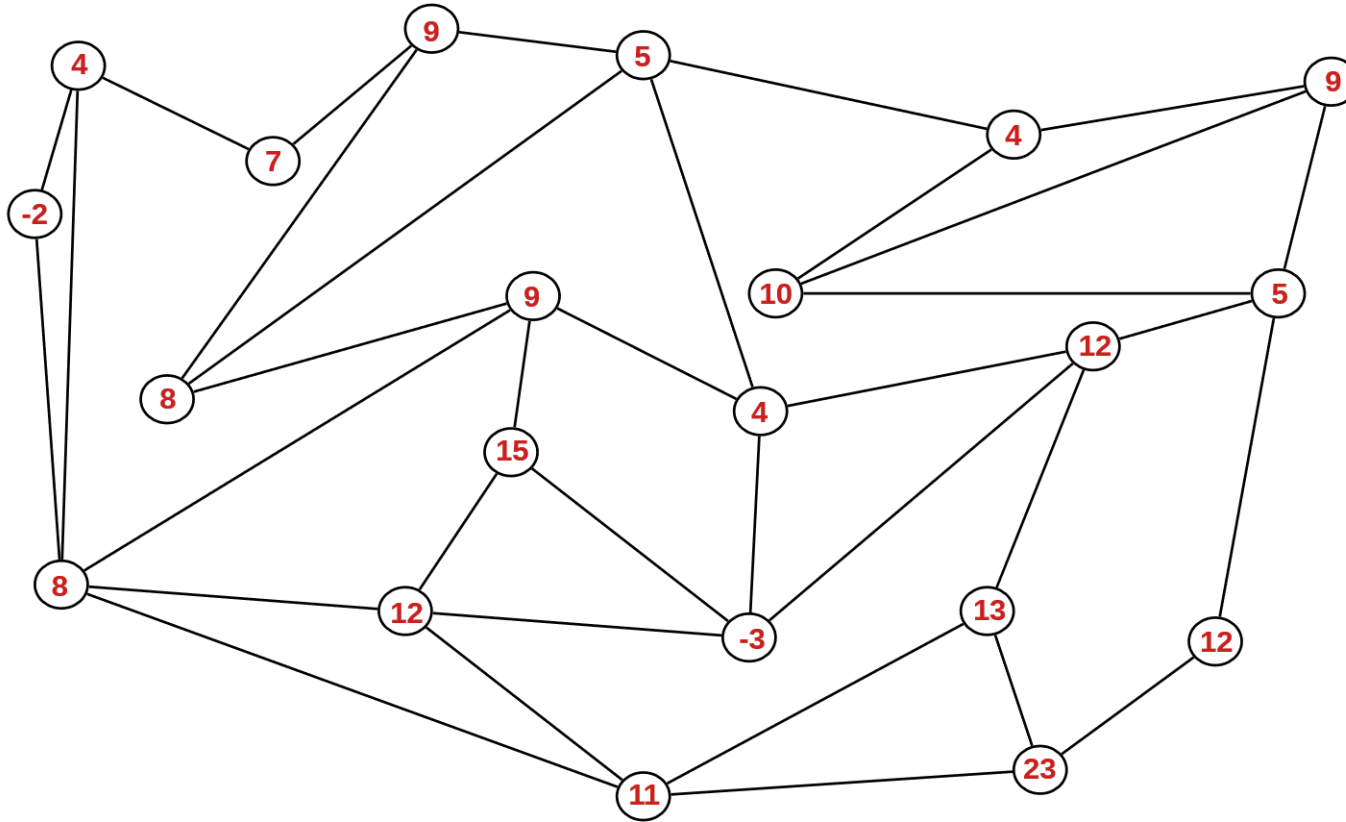


# Kid Krypto





# Kid Krypto





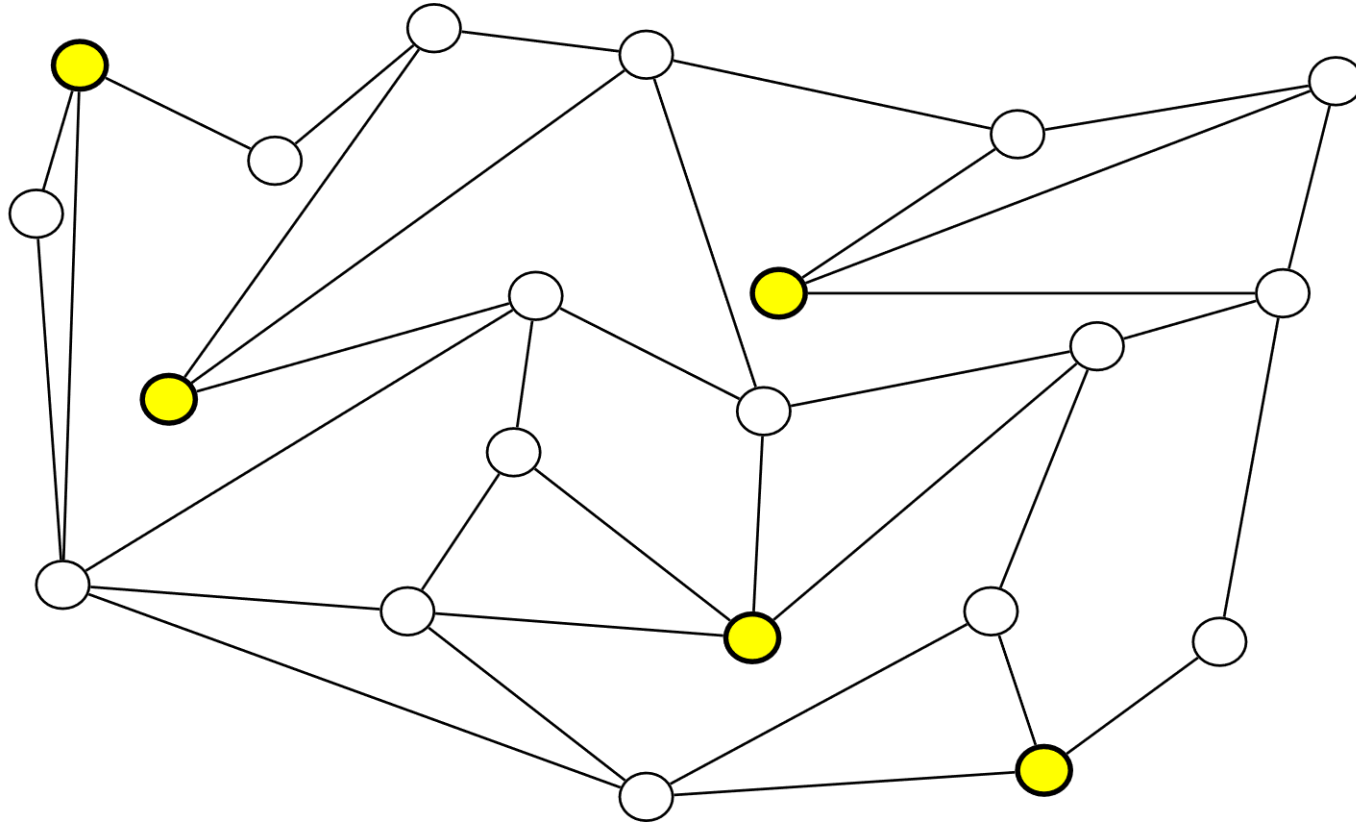
# Einwegfunktionen

Das Prinzip der Einwegfunktion ist anschaulich darzustellen.



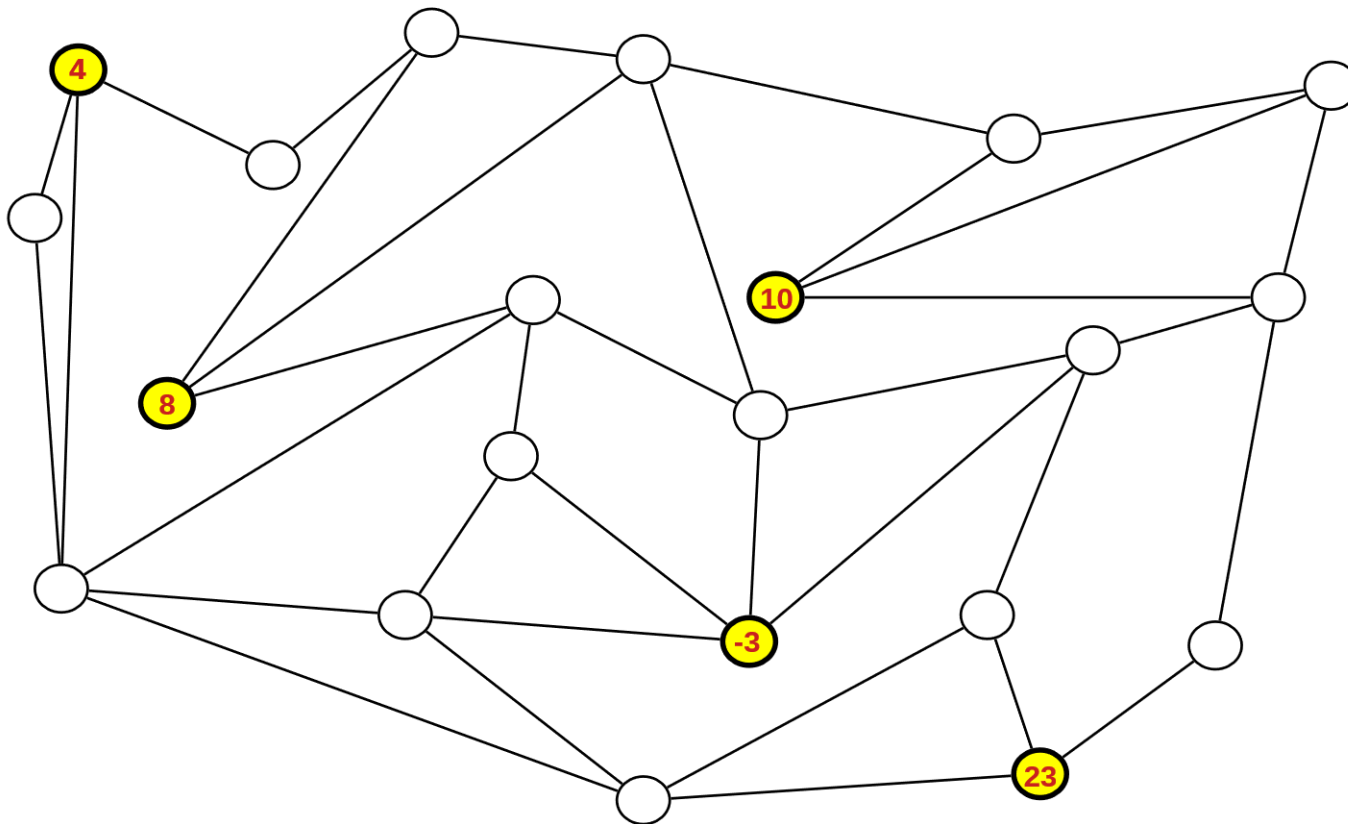


# Kid Krypto





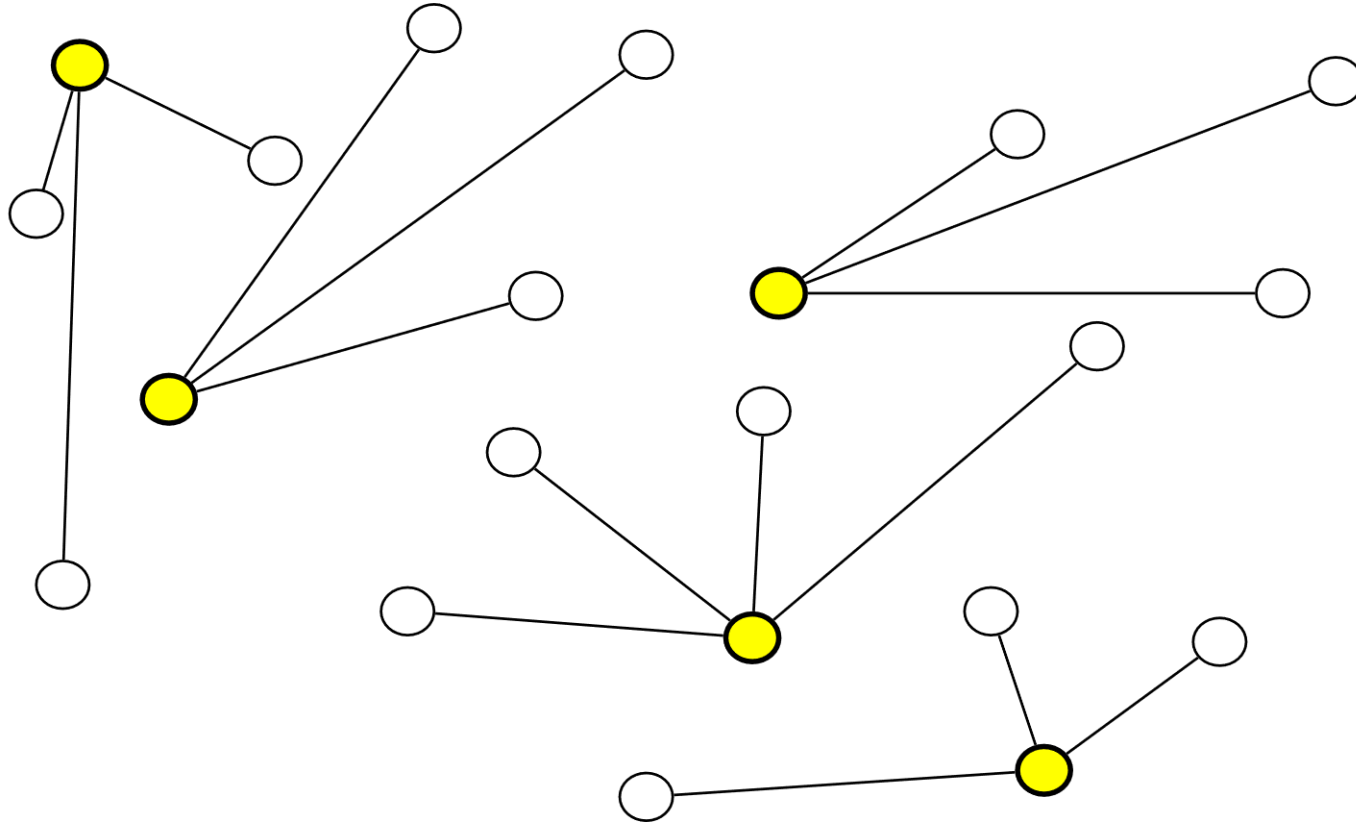
# Kid Krypto



$$\begin{array}{r} 4 \\ +10 \\ + 8 \\ - 3 \\ \hline +23 \\ 42 \end{array}$$



# Kid Krypto





# Hashing

Das Prinzip der Einwegfunktion ist anschaulich darzustellen.

- das Prinzip der Einwegfunktion anhand einer Hashfunktion erläutern

LK



```
7 public class Konto {  
8  
9     // Anfang Attribute  
10    private int nummer;  
11    private String art;  
12    private int saldo;  
13    private int hash;  
14    private boolean angemeldet;  
15    private Kunde inhaber;  
16    // Ende Attribute  
17
```

```
18    /**  
19     * Konstruktor für Objekte der Klasse Konto  
20     * @param pNummer Kontonummer  
21     * @param pSaldo Saldo  
22     * @param pArt Giro oder Spar  
23     * @param pInhaber  
24     */  
25    public Konto(int pNummer, int pSaldo, String pArt, Kunde pInhaber) {  
26        this.nummer = pNummer;  
27        this.saldo = pSaldo;  
28        this.art = pArt;  
29        this.inhaber = pInhaber;  
30        angemeldet = false;  
31        int pin = (int) ((9000) * Math.random() + 1000);  
32        System.out.println("Ihre PIN wurde generiert auf "+pin);  
33        this.hash = String.valueOf(pin).hashCode();  
34    }
```



# 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

$$s[0]*31^{(n-1)} + s[1]*31^{(n-2)} + \dots + s[n-1]$$

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:

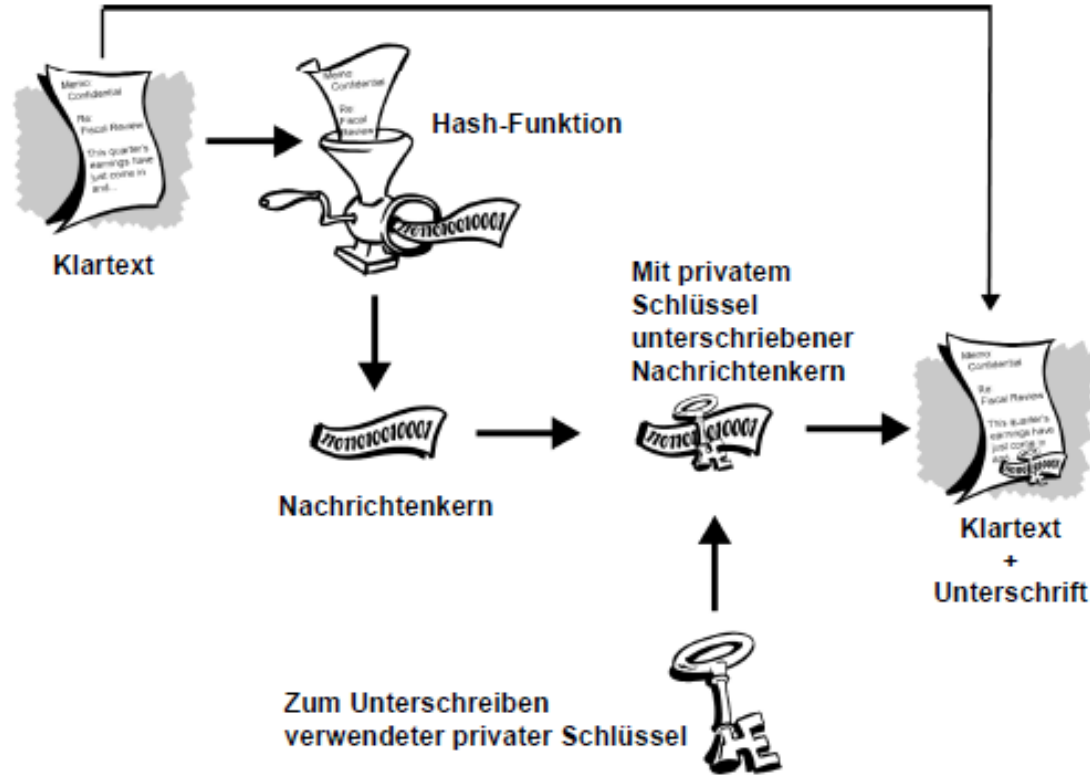
a hash code value for this object.



# Digitale Signatur



- die Prinzipien digital zertifizierter und signierter Daten erläutern

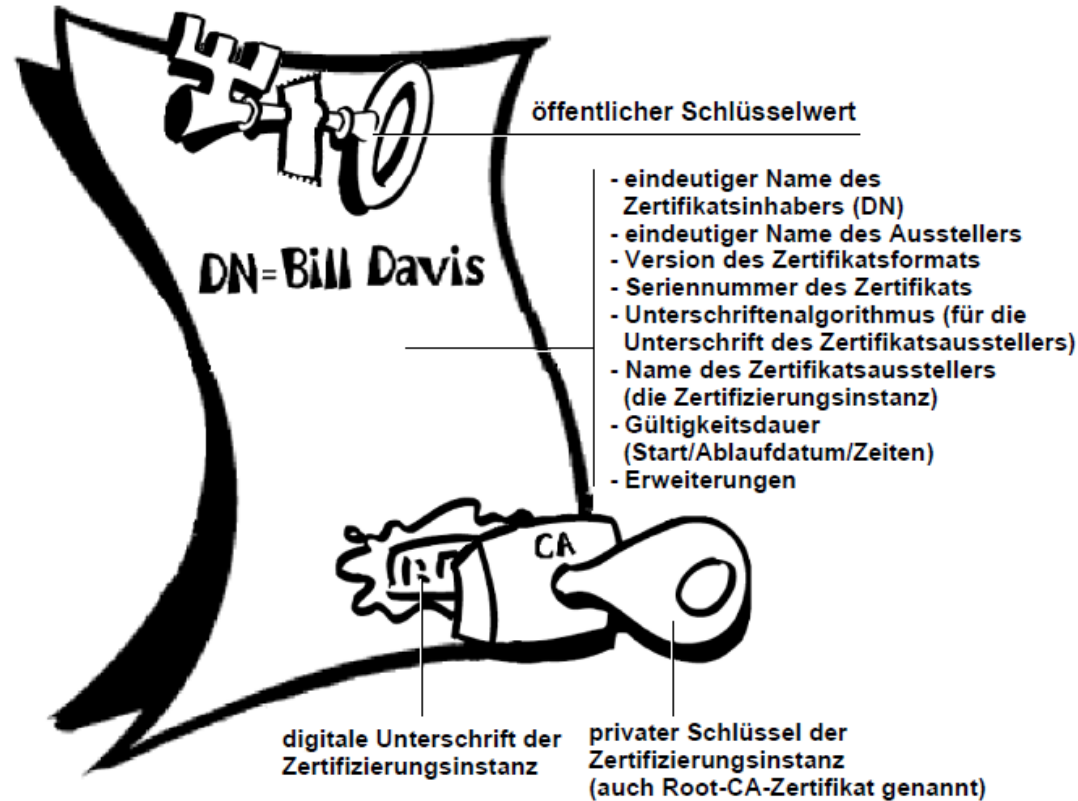


aus: Network Associates Inc. (Hrsg.): Handbuch „Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.



# 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**

1 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**

2 Alice prüft die Signatur und erhält

**BOB-AG.BGF BOB-AG.BGF**



# Verschlüsselung

- das Prinzip der hybriden Verschlüsselung LK 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 dazugehörige 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 ( $\approx 150'000$ ), alle Namen aus einem Telefonbuch ( $\approx 5'000'000$ ), 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  $\sim 50$  Giga MD5 Werte pro Sekunde ([Stand 2021](#)), um unsere Beispiel Rainbow-table zu erstellen braucht man also nur **0.4 Sekunden!**



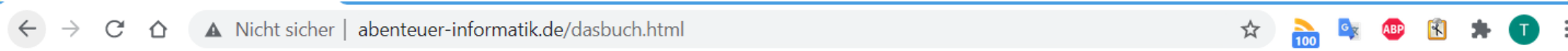
# Fragen



- 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



← → ↻ ↗ inf-schule.de/kryptologie/ 🔍 📱 ⚙️ 📧 📄 📌 📌 📌 📌 📌 📌

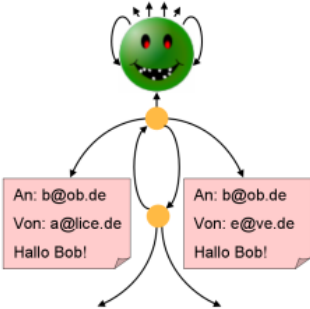
INF-SCHULE

11: Startseite / Kryptologie

## Kryptologie

### Worum geht es?

Wenn Daten zwischen Rechnern transportiert werden, können eine Reihe von Manipulationen vorgenommen werden. Kryptologie kommt immer dann ins Spiel, wenn solche Manipulationen verhindert bzw. aufgedeckt werden sollen und der Datenaustausch somit insgesamt sicherer gemacht werden soll. So kann eine Nachricht mit geeigneten kryptologischen Verfahren verschlüsselt oder auch digital signiert werden, bevor sie über unsichere Kanäle weitergeleitet wird.

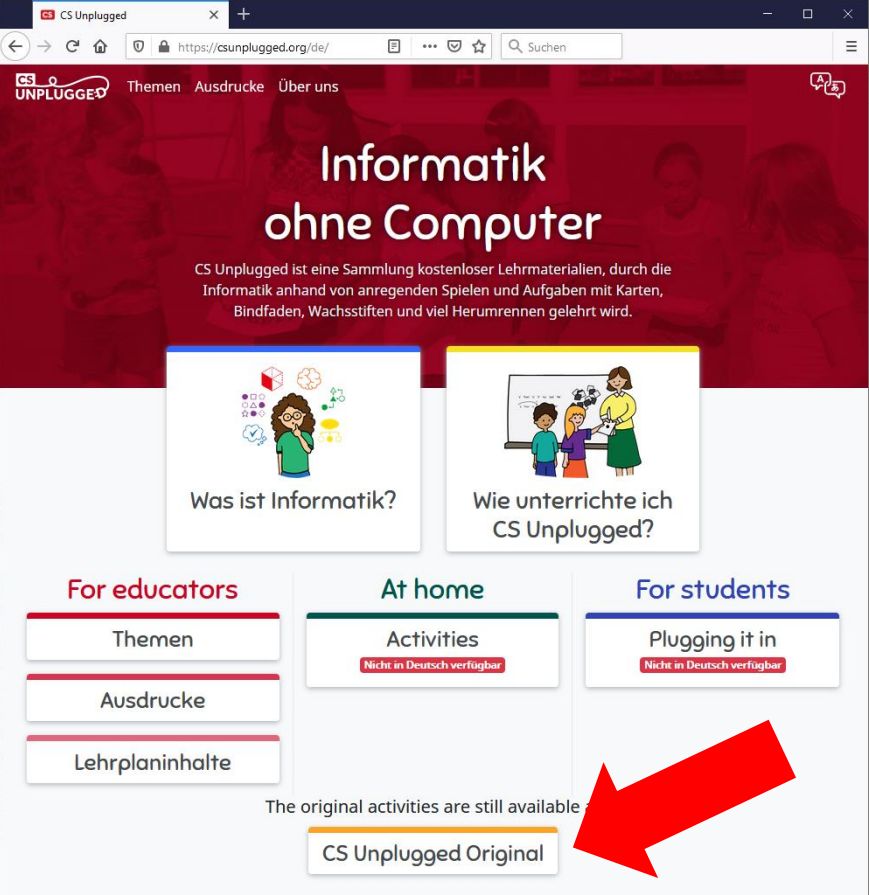


Wir werden uns hier mit kryptologischen Verfahren beschäftigen. Im Mittelpunkt werden dabei moderne Verfahren stehen, die derzeit in Kryptosystemen verwendet werden.

<https://t1p.de/6mof>



# Materialien



The screenshot shows the CS Unplugged website in German. The header includes the logo and navigation links: Themen, Ausdrücke, Über uns. The main heading is "Informatik ohne Computer". Below it, a paragraph explains that CS Unplugged is a collection of free teaching materials for learning computer science through games and tasks using cards, string, and other simple materials. Two large cards are featured: "Was ist Informatik?" with an illustration of a person thinking, and "Wie unterrichte ich CS Unplugged?" with an illustration of a teacher and students. Below these are three columns: "For educators" with links to Themen, Ausdrücke, and Lehrplaninhalte; "At home" with a link to Activities (marked "Nicht in Deutsch verfügbar"); and "For students" with a link to Plugging it in (marked "Nicht in Deutsch verfügbar"). At the bottom, a note states "The original activities are still available" with a link to "CS Unplugged Original", which is highlighted by a large red arrow.

<https://t1p.de/kmea8>



# Materialien



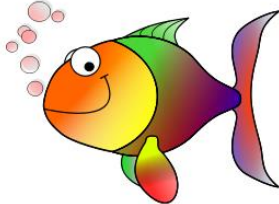
← → ↺ 🏠 martinstoeckli.ch/hash/de/index.php ☆ 🔍 📄 📱 📧 📧 📧 📧 📧 📧

← → Sicheres Speichern von Passwörtern • www.martinstoeckli.ch • 1/13

## Wie man mit Pfeffer den Fisch versalzt

Tutorial über das sichere Speichern von Passwörtern.

Author: Martin Stoeckli (aktualisiert 2021)

A cartoon illustration of a fish with a rainbow gradient body, orange head, and purple tail, blowing bubbles.

<https://t1p.de/h7de>



## 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

Alles außer Mathe

## Prüfungsaufgaben

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?
- ...?