Sicher kommunizieren

mithilfe der Kryptologie

Ziele des Workshops

Inhalte des WS

Sachanalyse

Sicher kommunizieren? Wozu?

▼

Informatische Konzepte!

Did.-meth. Überlegungen

Unterrichtsmaterial

▼

Bücher/Handreichungen

Enaktiv-haptische Übungen

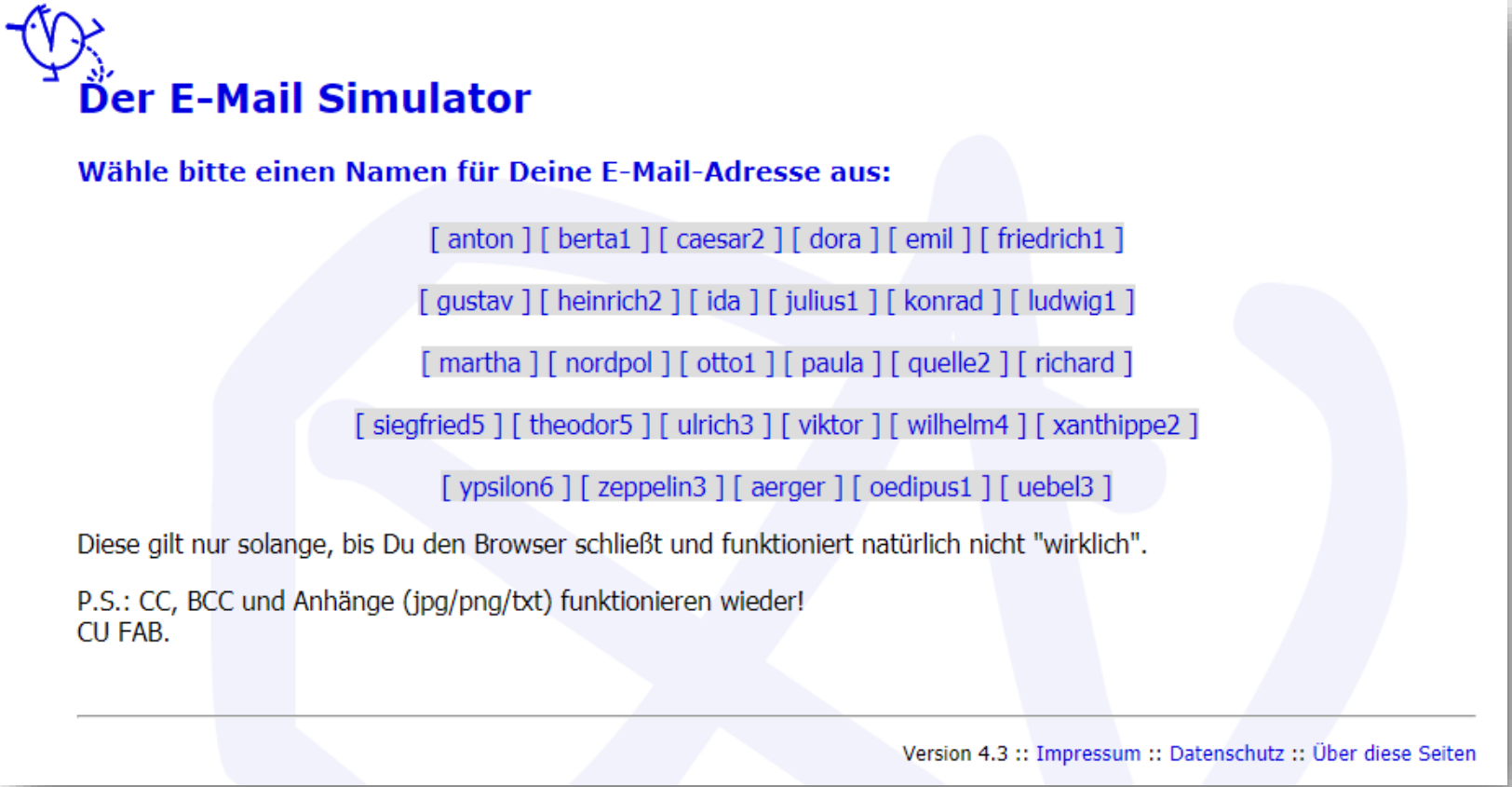
Rahmenplan Klasse 6

In der vernetzten Welt kommunizieren [MD] [BO] [DRF] **ca. 8 Unterrichtsstunden**

Kenntnisse über elementare Prinzipien des Internets sind für die effektive und reflektierte Nutzung von Kommunikationsdiensten unerlässlich.

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
mithilfe eines Internetdienstes kommunizieren • Nachrichten unter Angabe eines geeigneten Betreffs an einen oder mehrere Empfänger versenden • Anhänge hinzufügen und speichern	Ein geeigneter Dienst ist die E-Mail. Neuerstellung, Beantwortung und Weiterleitung sind Möglichkeiten des Versendens von Nachrichten. Die Schülerinnen und Schüler können die Dateigröße in der Maßeinheit Byte mit Präfixen und den Dateityp angeben.
• Authentizität und Gefahrenpotential von eingehenden Nachrichten abschätzen	Die Beurteilung erfolgt anhand der Absenderadresse, des Betreffs oder des Inhalts. Die Schülerinnen und Schüler reagieren in geeigneter Weise.
• mit personenbezogenen Daten verantwortungsbewusst umgehen	Die Schülerinnen und Schüler beachten sowohl den Schutz der eigenen Daten als auch den

Mini-Mehl oder MailKids



Der E-Mail Simulator

Wähle bitte einen Namen für Deine E-Mail-Adresse aus:

[anton] [berta1] [caesar2] [dora] [emil] [friedrich1]

[gustav] [heinrich2] [ida] [julius1] [konrad] [ludwig1]

[martha] [nordpol] [otto1] [paula] [quelle2] [richard]

[siegfried5] [theodor5] [ulrich3] [viktor] [wilhelm4] [xanthippe2]

[ypsilon6] [zeppelin3] [aerger] [oedipus1] [uebel3]

Diese gilt nur solange, bis Du den Browser schließt und funktioniert natürlich nicht "wirklich".

P.S.: CC, BCC und Anhänge (jpg/png/txt) funktionieren wieder!
CU FAB.

Version 4.3 :: Impressum :: Datenschutz :: Über diese Seiten

Rahmenplan Klasse 7

Sicher kommunizieren [MD] [BO] [DRF] [PG] **ca. 8 Unterrichtsstunden**

Die Gewährleistung der Vertraulichkeit ist eine Notwendigkeit für die Kommunikation im Internet und für die Sicherung der Privatsphäre.

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
Verschlüsselung verstehen • klassische Verfahren der symmetrischen Verschlüsselung anschaulich erläutern • kurze Nachrichten verschlüsselt austauschen Vertraulichkeit herstellen	Verschlüsselung ist eine Codierung, bei der die Decodierung für Außenstehende nicht möglich sein soll. Die Schülerinnen und Schüler beschreiben klassische Verfahren unter Verwendung der Begriffe Klartext- und Geheimtextalphabet, Klartext und Geheimtext, Schlüssel, Verschlüsseln und Entschlüsseln. Sie erkennen, dass durch Verschlüsselung eine vertrauliche Kommunikation ermöglicht wird. Die Schülerinnen und Schüler argumentieren zur Sicherheit der Verfahren.

Rahmenplan Klasse 9 Gy

Prinzipien der Datenübertragung verstehen [MD] [BO] [DRF] **ca. 10 Unterrichtsstunden**

Die Schülerinnen und Schüler erweitern ihre Vorstellungen von Struktur und Arbeitsweise des Internets, um Konsequenzen der Übermittlung von Daten und Metadaten einschätzen und Schlussfolgerungen ableiten zu können.

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
grundlegende Prinzipien der Datenübertragung im Internet beschreiben	Die Prinzipien sind anschaulich und enaktiv-haptisch zu vermitteln.
• Prinzip der asymmetrischen Verschlüsselung	Die asymmetrische Verschlüsselung wird zur Sicherung der Vertraulichkeit, Authentizität und Integrität eingesetzt.
Codierung verstehen • Prinzip der Codierung erläutern	Ausgehend von der Übertragung einer Nachricht werden ASCII und Unicode thematisiert. Die Schülerinnen und Schüler stellen einen Transfer zu Codierungsverfahren aus verschie-

Rahmenplan Klasse 10 RegS

Digitalisierung in meiner Umgebung untersuchen **ca. 20 Unterrichtsstunden**

[MD] [BO] [BNE] [DRF] [PG]

ca. 12 Unterrichtsstunden

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
• Prinzip der asymmetrischen Verschlüsselung hinsichtlich Integrität, Vertraulichkeit und Authentizität untersuchen	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.

Informatische Konzepte

- Klassische symmetrische Verschlüsselungsverfahren
- Prinzip der asymmetrischen Verschlüsselung
- Klartext, Geheimtext, Klartextalphabet, Geheimtextalphabet
- (privater/öffentlicher) Schlüssel
- Vertraulichkeit
- Integrität
- Authentizität
- Verbindlichkeit*
- Geschichte der Informatik*

*optional

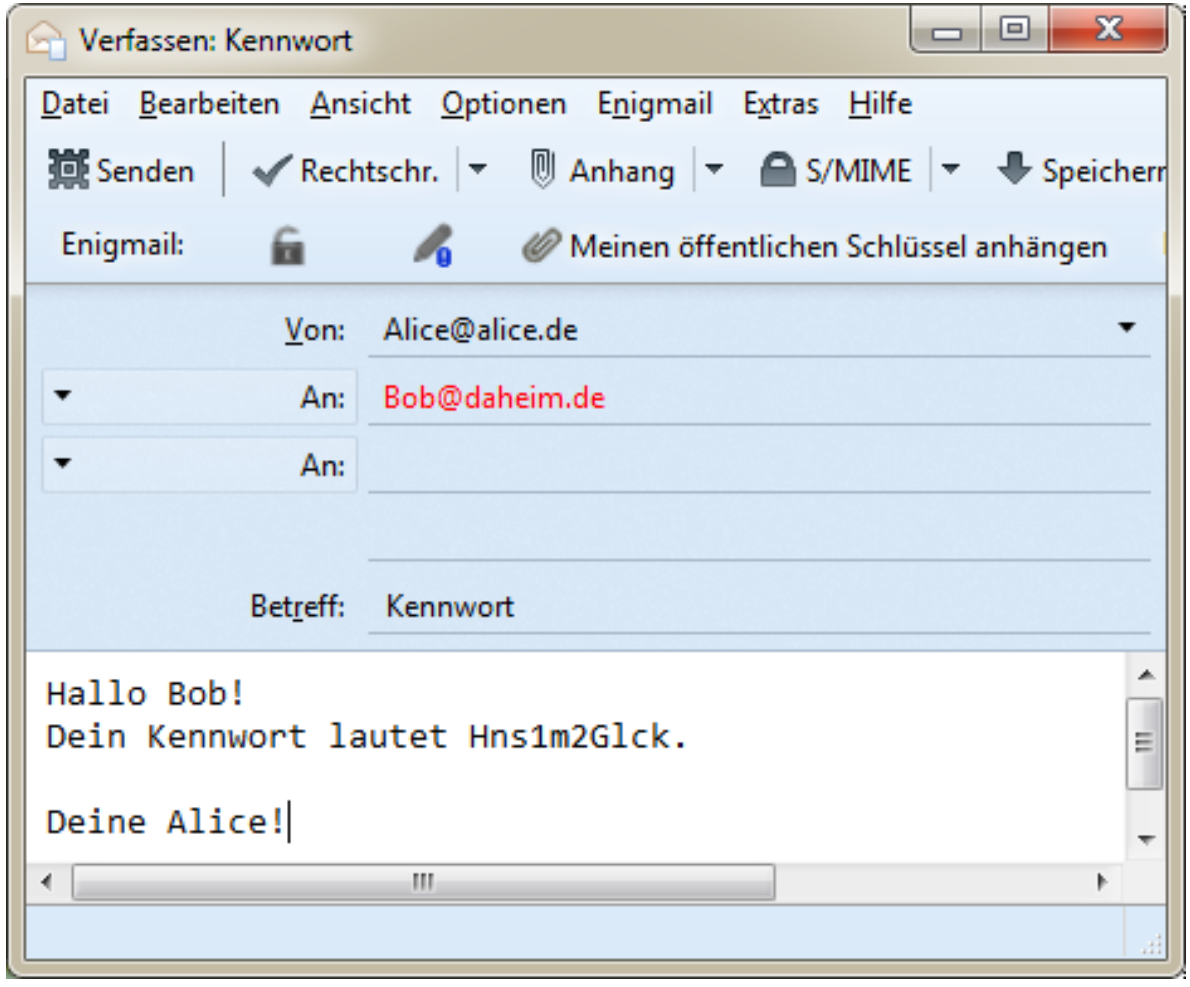
Hallo Bob!

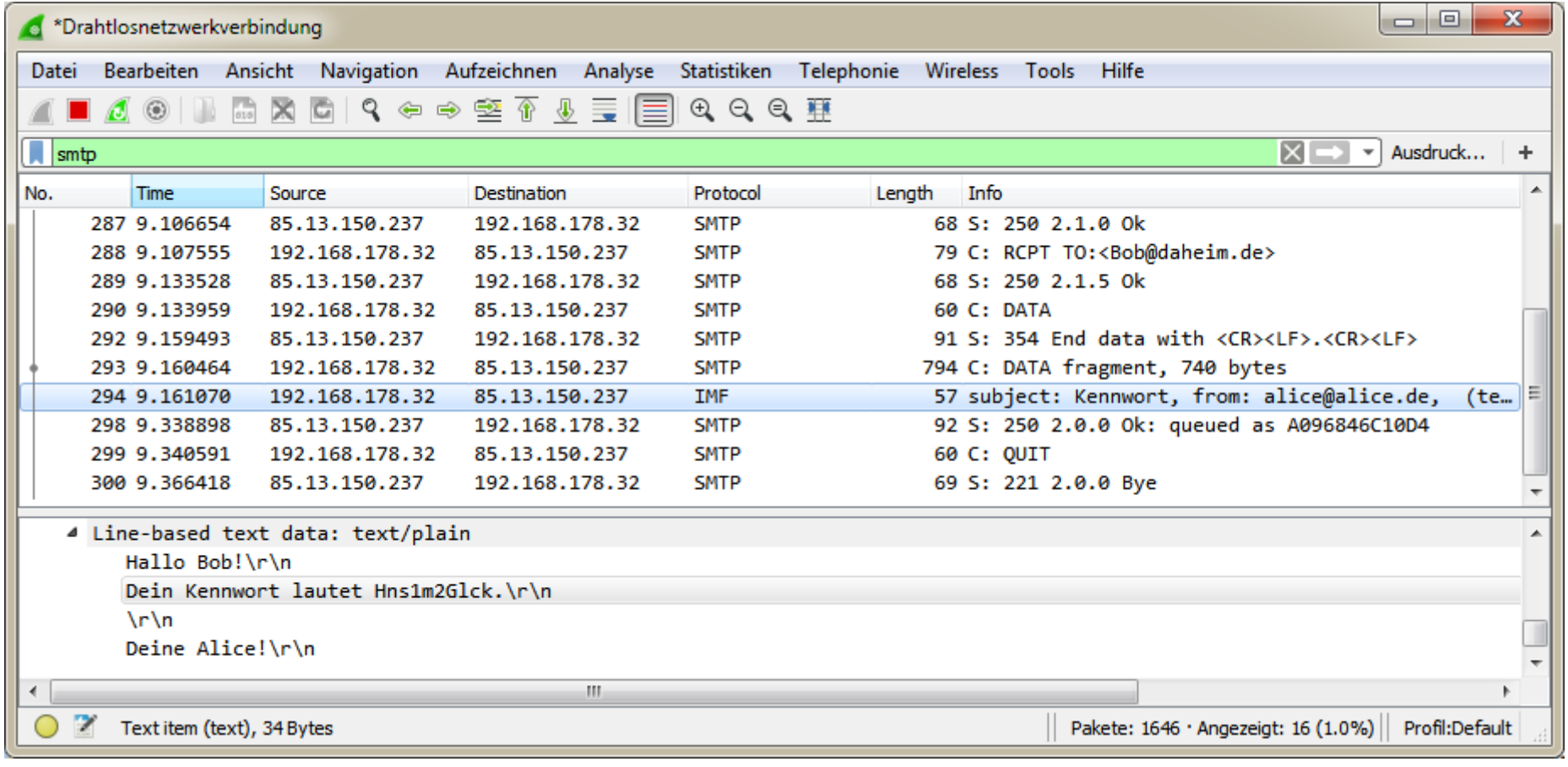
Dein Kennwort lautet

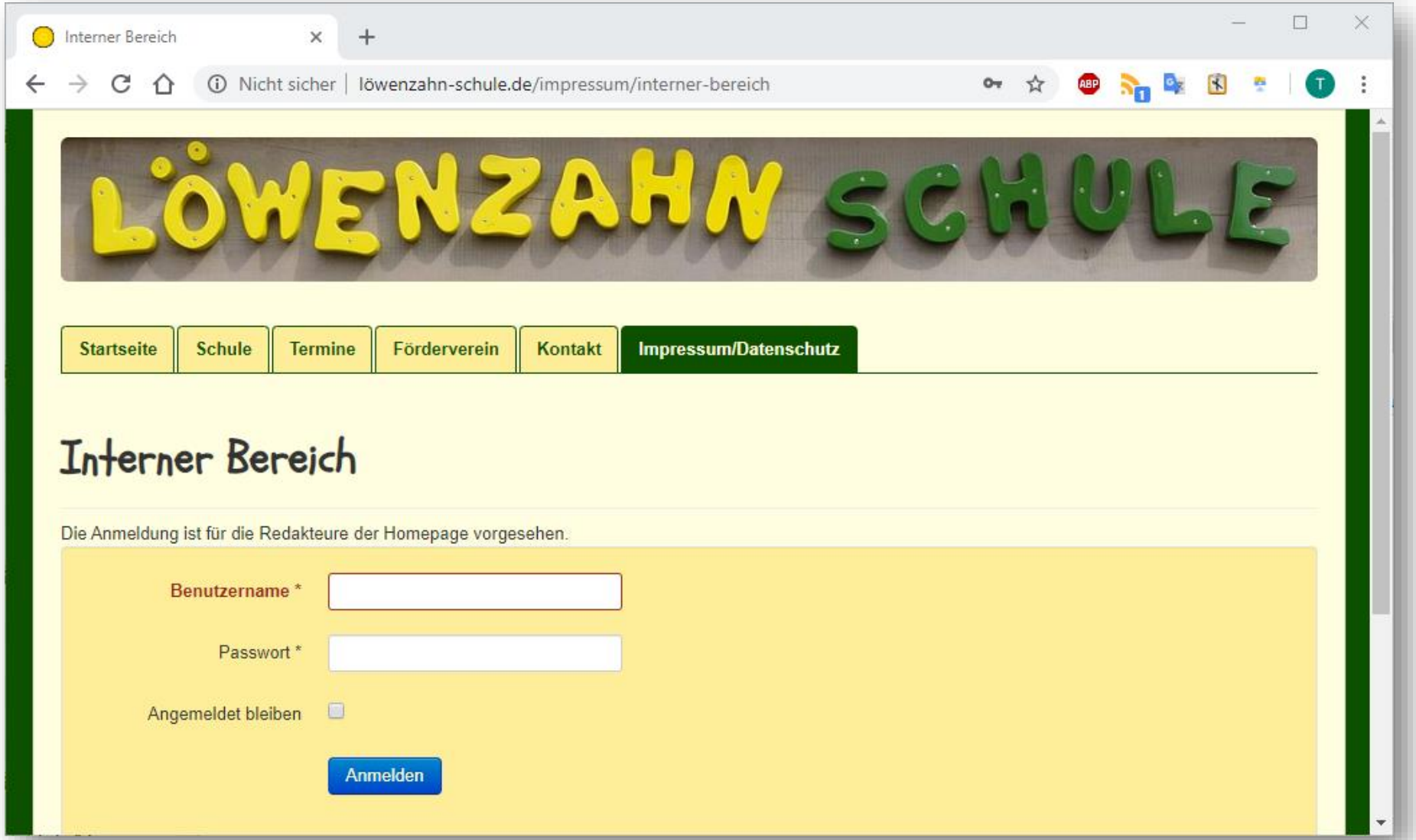
Hns1m2Glck.

Deine Alice!

Hallo Bob!
Das Kennwort lautet
Hns1m2Glck.


Verfassen: Kennwort
Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe
Senden
Rechtschr.
Anhang
S/MIME
Speicherr
Enigmail:
Meinen öffentlichen Schlüssel anhängen
Von:
Alice@alice.de
An:
Bob@daheim.de
An:
Betreff:
Kennwort
Hallo Bob!
Dein Kennwort lautet Hns1m2Glck.
Deine Alice!


*Drahtlosnetzwerkverbindung
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
smtp
Ausdruck...
No. Time Source Destination Protocol Length Info
287 9.106654 85.13.150.237 192.168.178.32 SMTP 68 S: 250 2.1.0 Ok
288 9.107555 192.168.178.32 85.13.150.237 SMTP 79 C: RCPT TO:<Bob@daheim.de>
289 9.133528 85.13.150.237 192.168.178.32 SMTP 68 S: 250 2.1.5 Ok
290 9.133959 192.168.178.32 85.13.150.237 SMTP 60 C: DATA
292 9.159493 85.13.150.237 192.168.178.32 SMTP 91 S: 354 End data with <CR><LF>.<CR><LF>
293 9.160464 192.168.178.32 85.13.150.237 SMTP 794 C: DATA fragment, 740 bytes
294 9.161070 192.168.178.32 85.13.150.237 IMF 57 subject: Kennwort, from: alice@alice.de, (te…
298 9.338898 85.13.150.237 192.168.178.32 SMTP 92 S: 250 2.0.0 Ok: queued as A096846C10D4
299 9.340591 192.168.178.32 85.13.150.237 SMTP 60 C: QUIT
300 9.366418 85.13.150.237 192.168.178.32 SMTP 69 S: 221 2.0.0 Bye
Line-based text data: text/plain
Hallo Bob!\r\n
Dein Kennwort lautet Hns1m2Glck.\r\n
\r\n
Deine Alice!\r\n
Text item (text), 34 Bytes
Pakete: 1646 · Angezeigt: 16 (1.0%)
Profil:Default

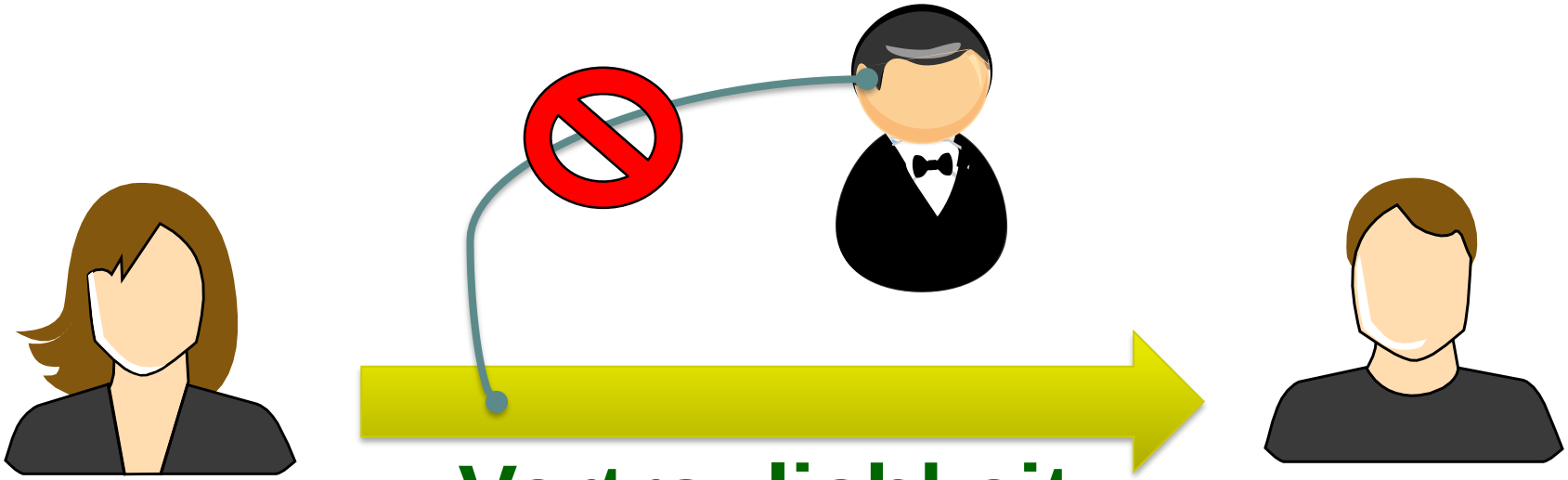

Interner Bereich
Nicht sicher | löwenzahn-schule.de/impressum/interner-bereich
LÖWENZAHN SCHULE
Startseite
Schule
Termine
Förderverein
Kontakt
Impressum/Datenschutz
Interner Bereich
Die Anmeldung ist für die Redakteure der Homepage vorgesehen.
Benutzername *
Passwort *
Angemeldet bleiben
Anmelden

Alle Themen
Programmieren lernen
Gymnasium
Bei Serlo-Informatik mitarbeiten
Newsletter

Sicher Kommunizieren - Einfach erklärt

Das letzte von fünf Videos von Alexander Lehmann zum Thema Verschlüsselung und Datenschutz.

Sicherheitsziele

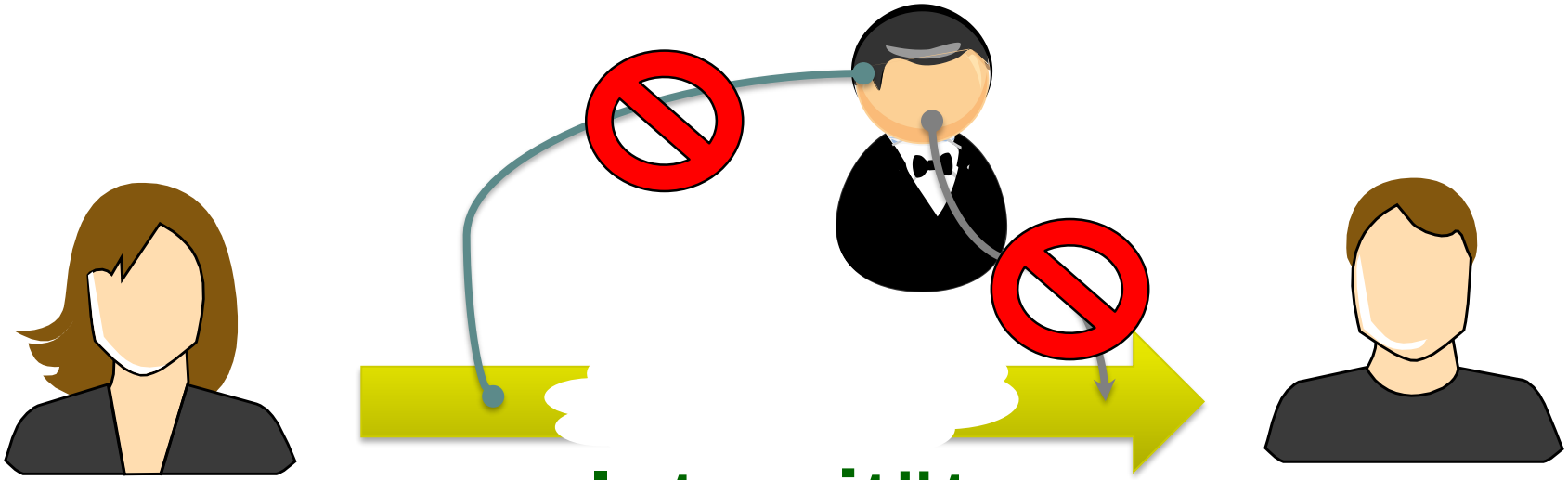


Vertraulichkeit

kein Mitlesen durch Fremde

Verschlüsselung

Sicherheitsziele

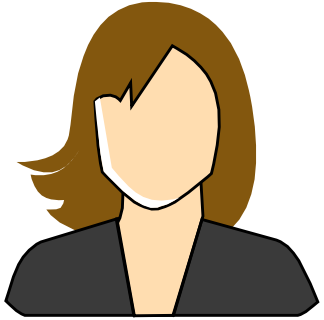


Integrität

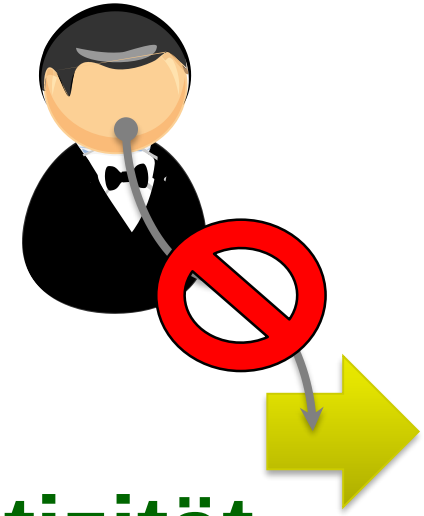
keine Manipulation durch Fremde

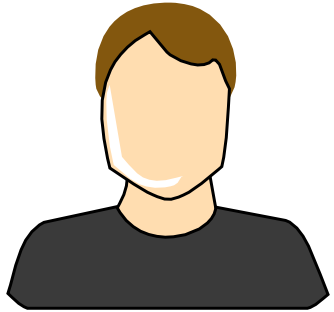
Versiegelter Brief

Sicherheitsziele



Alice





Bob

Authentizität

Nachricht ist definitiv vom Absender

Digitale Unterschrift

Sicherheitsziele

Verbindlichkeit

Keiner kann seine Urheberschaft bestreiten

Digitale Unterschrift

Grundbegriffe

Kryptologie/Kryptografie/Kryptoanalyse

Grundbegriffe

Klartext-/Geheimtext

Klartext-/Geheimtextalphabet

Grundbegriffe

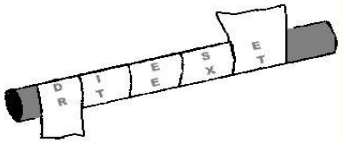
Schlüssel

Klassische Verschlüsselung

Steganographie
(verstecken)

Kryptographie
(verschlüsseln)

Substitution

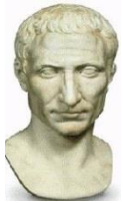


Transposition

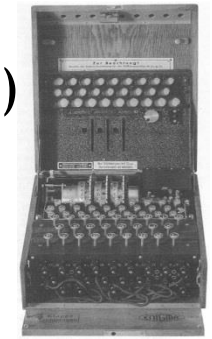
Chiffrierung
(Buchstaben ersetzen)

Codierung
(Wörter ersetzen)

Monoalphabetisch
(Captain Kidd, Caesar)



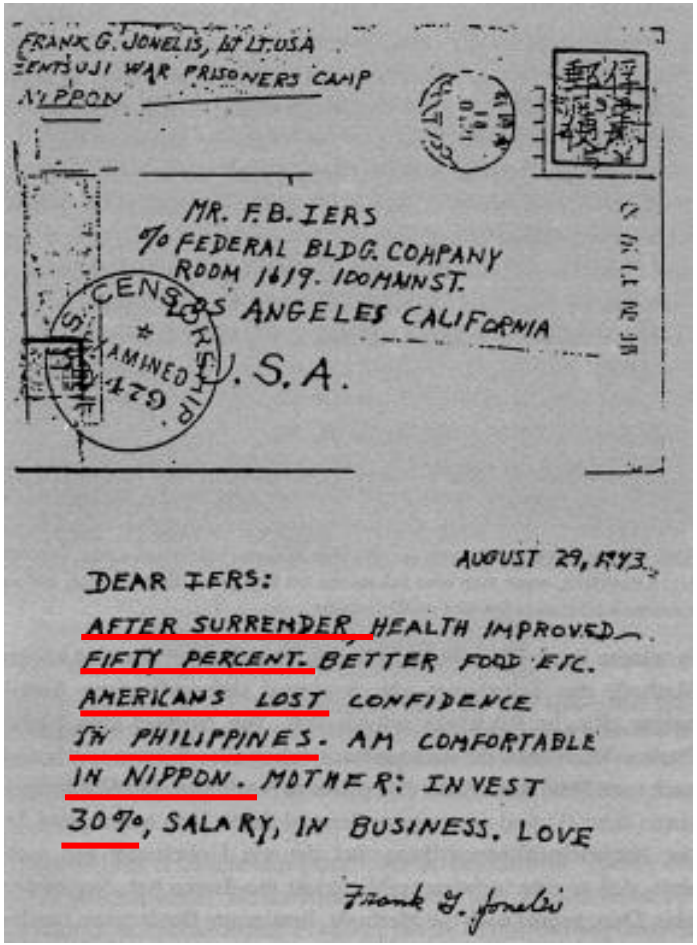
Polyalphabetisch
(Vigenère, Enigma)



one time pad

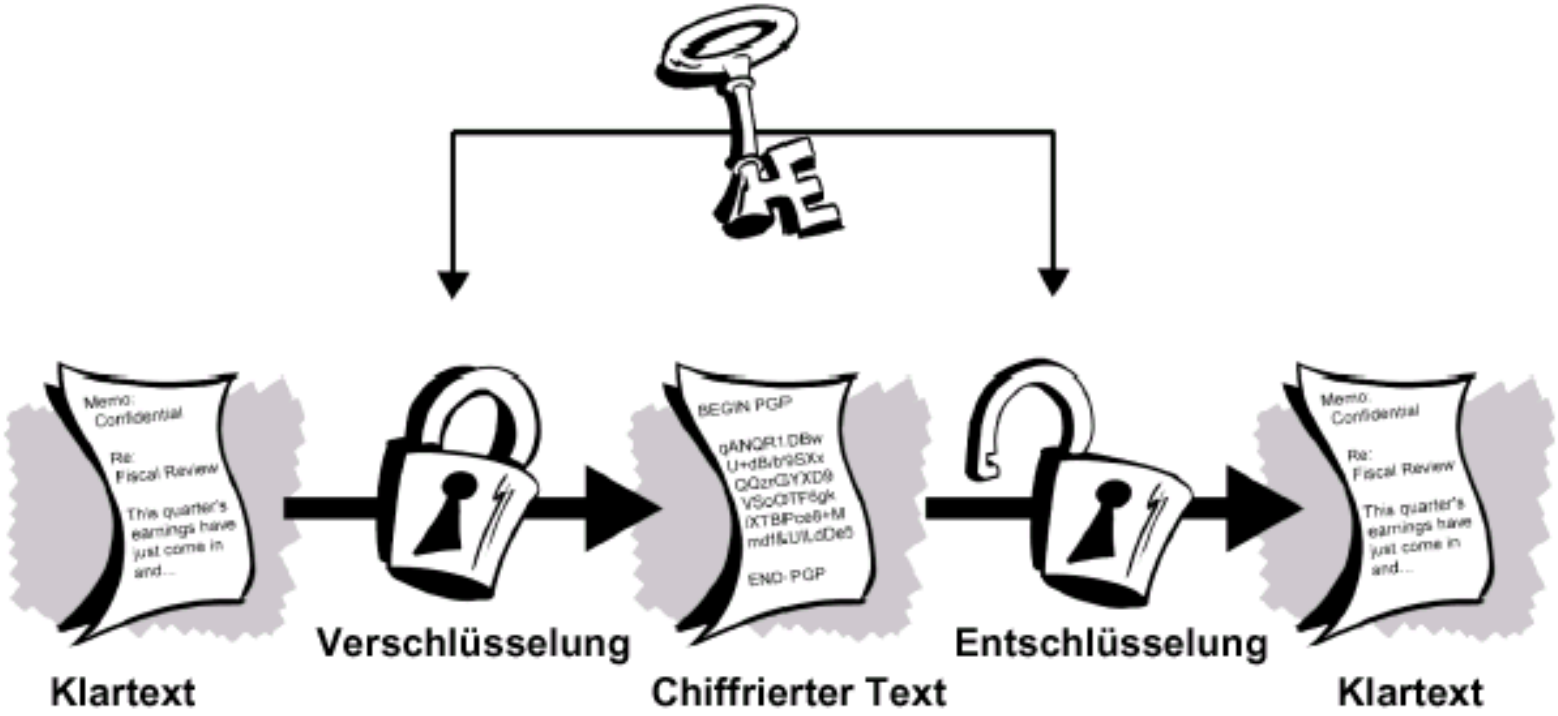
Steganografie

- Eine „harmlose“ Karte eines amerikanischen Kriegsgefangene in Japan...
- ... enthielt Informationen über amerikanische Verluste. (ersten zwei Wörter einer Zeile)



Quelle:
Kippenhahn, R.: Verschlüsselte Botschaften, S.39.

Symmetrische Verfahren



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

Stationsbetrieb

Station 1: Skytale und FLEIßNER-Schablone

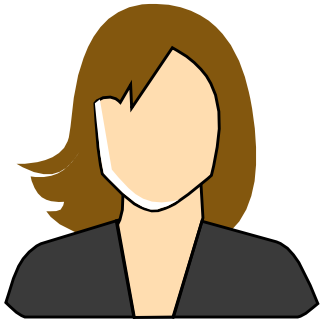
Station 2: CAESAR und Co.

Station 3: POLYBIOS und PLAYFAIR

Station 4: VIGENÈRE und 100 % (erst nach 2)

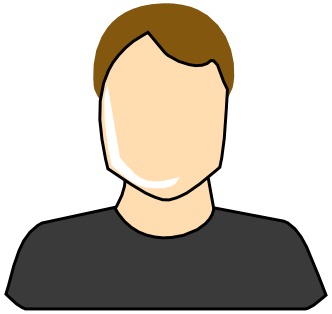
Station 5: Enigma (nur für Freaks!)

Grundproblem aller Verfahren



Alice

Mr. X



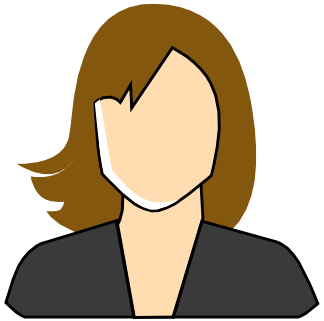
Bob

Hallo Bob!
Dein Schlüssel lautet
Hns1m2Glck.

Deine Alice!

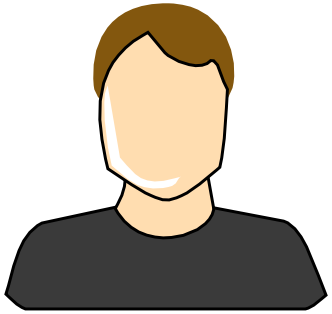
Monoalphabetisch → statistische Angriffe

Grundproblem aller Verfahren



Alice

Mr. X



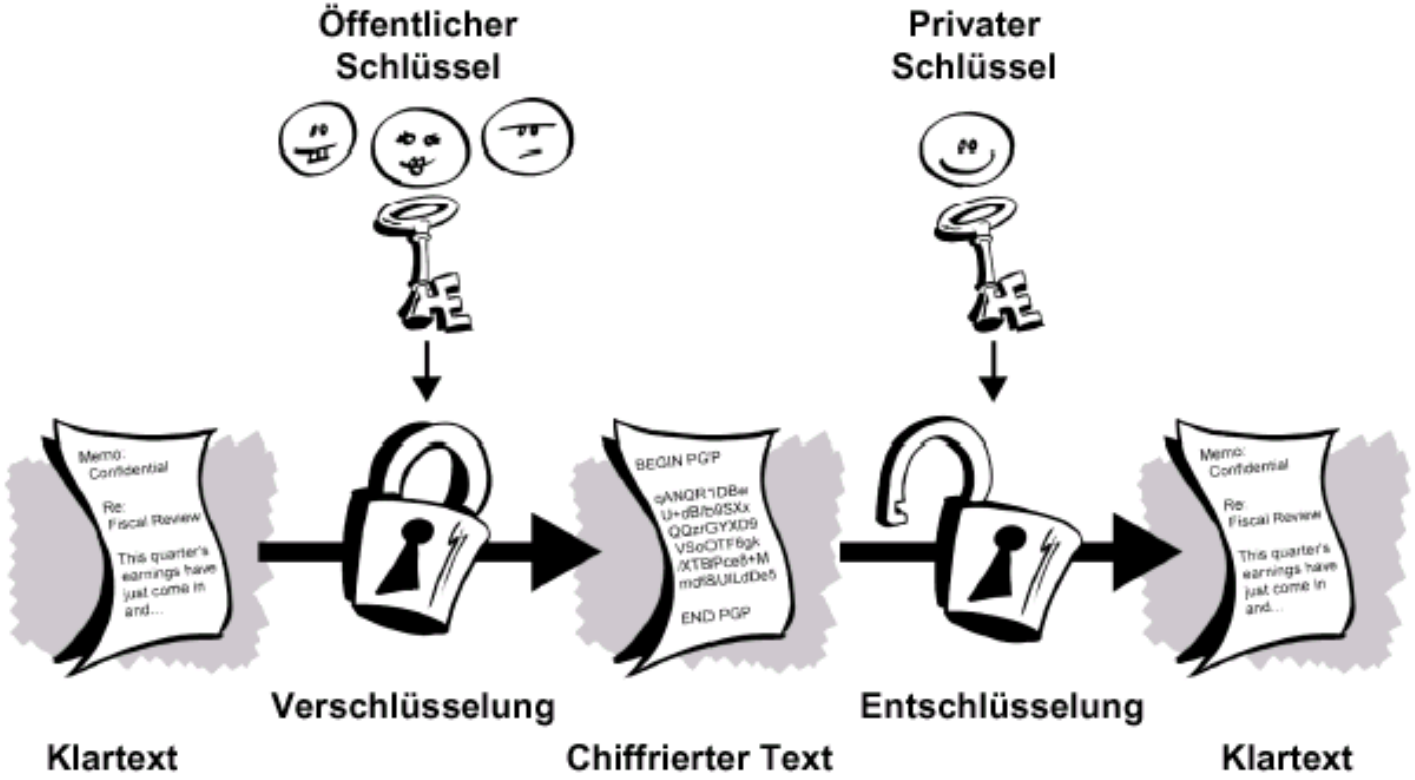
Bob

Hallo Bob!
Dein Schlüssel lautet
Hns1m2Glck.

Deine Alice!

Schlüsseltausch

Asymmetrische Verfahren



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

Asymmetrische Verfahren

Werkzeug ASYM-Kodierer

Prüfe die Behauptung:

Der Klartext `EC-CARD` wurde mit dem Schlüssel `AZS` zum Geheimtext `JVQFQUH`.

Variante A:

Verschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Klartext	E	C	-	C	A	R	D
Geheimtext							

Variante B:

Entschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Geheimtext	J	V	Q	F	Q	U	H
Klartext							

Werkzeug ASYM-Kodierer

Prüfe die Behauptung:

Der Klartext `EC-CARD` wurde mit dem Schlüssel `AZS` zum Geheimtext `JVQFQUH`.

Variante A:

Verschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Klartext	E	C	-	C	A	R	D
Geheimtext	J	V	Q	F	Q	U	H

Variante B:

Entschlüsseln							
Schlüssel	A	Z	S	A	Z	S	A
Geheimtext	J	V	Q	F	Q	U	H
Klartext	T	Z	O	L	.	J	P

Werkzeug ASYM-Kodierer

aus Gallenbacher. Abenteuer Informatik

Prüfe die Behauptung:

Der Klartext `EC-CARD` wurde mit dem Schlüssel `AZS` zum Geheimtext `JVQFQUH`.

... und was passiert beim Schlüssel `PCT`?

Verschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Klartext	E	C	-	C	A	R	D
Geheimtext							

Entschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Geheimtext	J	V	Q	F	Q	U	H
Klartext							

Werkzeug ASYM-Kodierer

Prüfe die Behauptung:

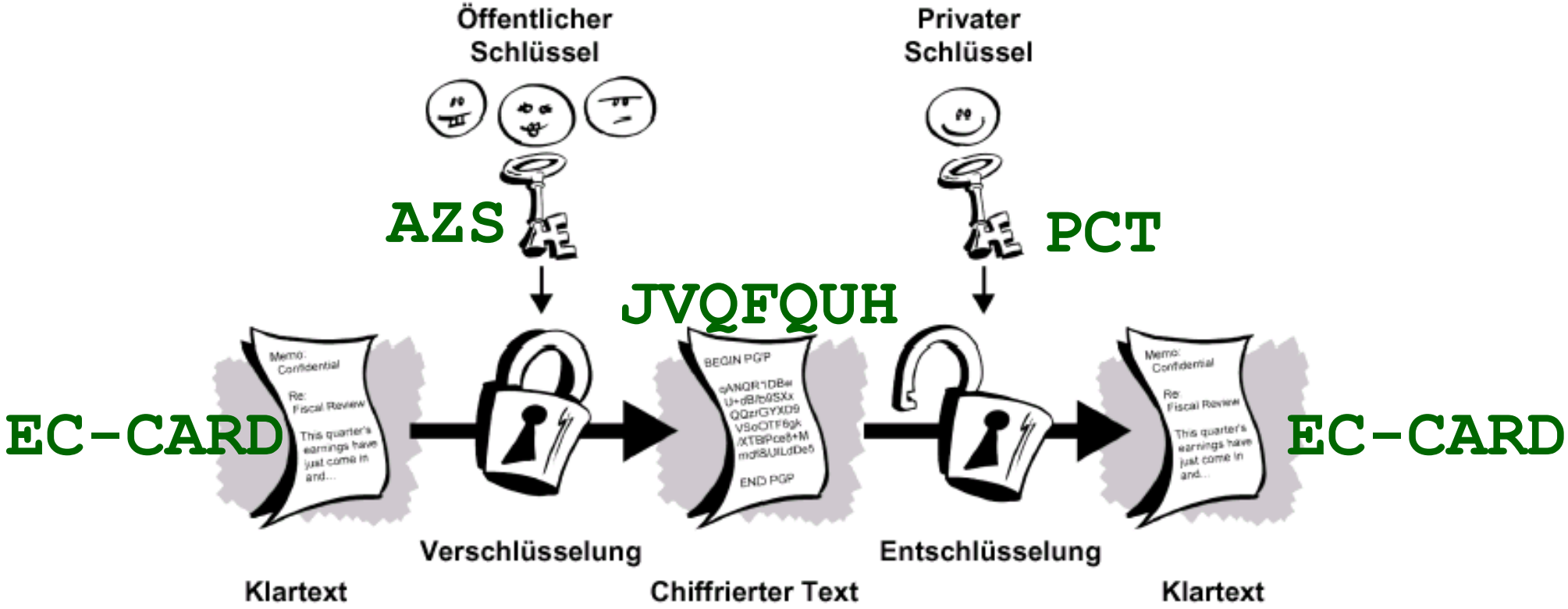
Der Klartext `EC-CARD` wurde mit dem Schlüssel `AZS` zum Geheimtext `JVQFQUH`.

... und was passiert beim Schlüssel `PCT`?

Verschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Klartext	E	C	-	C	A	R	D
Geheimtext	Q	G	S	P	L	C	B

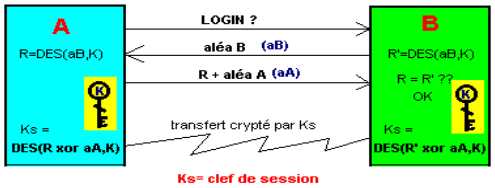
Entschlüsseln							
Schlüssel	P	C	T	P	C	T	P
Geheimtext	J	V	Q	F	Q	U	H
Klartext	E	C	-	C	A	R	D

Asymmetrische Verfahren

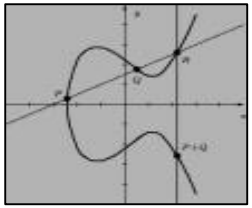


aus: Network Associates Inc. (Hrsg.): Handbuch "Einführung in die Kryptographie", Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf".

Aktuelle Verfahren

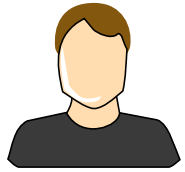


moderne computergestützte Verfahren

- symmetrisch (geheimer Schlüssel)
  - Blockchiffrier-algorithmen
    - DES
    - 
  - Stromchiffrier-algorithmen
    - AES - WPA2
    - 
- asymmetrisch (Public Key, Diffie u. Hellmann)
  - RSA (Rivest, Shamir, Adleman)
    - 
  - El Gamal
    - 
  - Elliptische Kurven
    - 

Asymmetrische Verfahren

Alice **BGF**



Bob-AG

```
+: BGF
-: FDB
```

1. Alice fragt Bob-AG nach deren public key

⟶ Bob-AG antwortet mit **BGF**

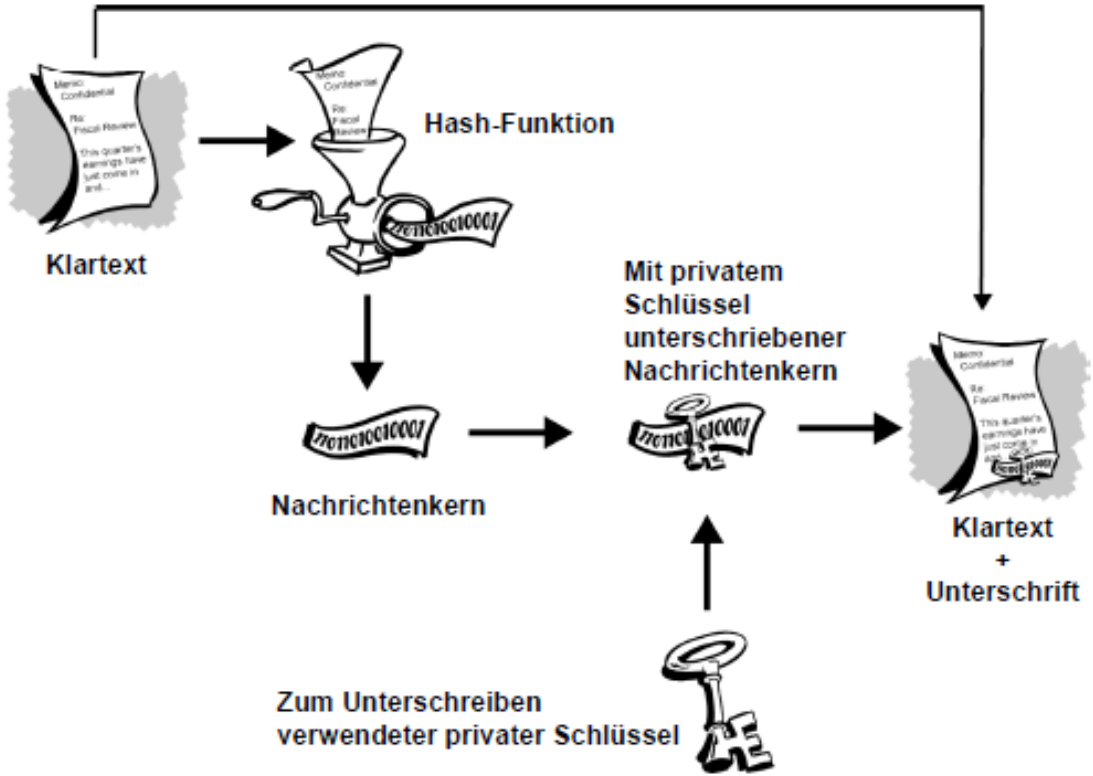
2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG

⟶ Bob-AG entschlüsselt: **ACHTEINS**

3. Alice erhält **OK H.** und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis **OK = OK**

⟵ Bob-AG verschlüsselt Bestätigung **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**

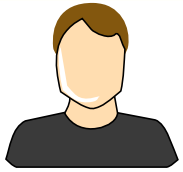
Digitale Signatur



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

Asymmetrische Verfahren

Alice **BGF**



Bob-AG

```
+: BGF
-: FDB
```

1. Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG

Bob-AG entschlüsselt: **ACHTEINS**

Bob-AG verschlüsselt Bestätigung **OK** mit private key zu **H.**

und sendet **OK** sowie das verschlüsselte **OK**

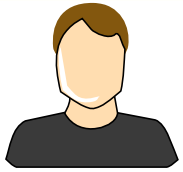
3. Alice erhält **OK H.**

und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis

OK = OK

Asymmetrische Verfahren

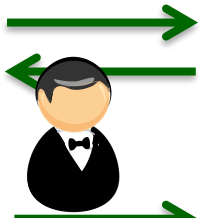
Alice **BGF**



Bob-AG

```
+: BGF
-: FDB
```

1. Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit **BGF**

2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG

Bob-AG entschlüsselt: **ACHTEINS**

Bob-AG verschlüsselt Bestätigung **OK** mit private key zu **H.**

und sendet **OK** sowie das verschlüsselte **OK**

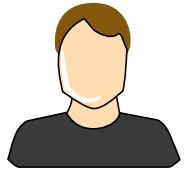
3. Alice erhält **OK H.**

und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis

OK = OK

Asymmetrische Verfahren

Alice **BGF**



Bob-AG

+: BGF
−: FDB

1. Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG

Bob-AG entschlüsselt: **ACHTEINS**

Bob-AG verschlüsselt Bestätigung **OK** mit private key zu **H.**

und sendet **OK** sowie das verschlüsselte **OK**

3. Alice erhält **OK H.**

und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis

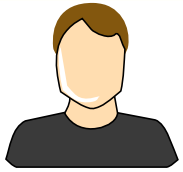
OK = OK

Asymmetrische Verfahren

Alice **CEF**

+: CEF
−: ZLB

BGF



Bob-AG

+: BGF
−: FDB

❶ Alice fragt Bob-AG nach deren public key

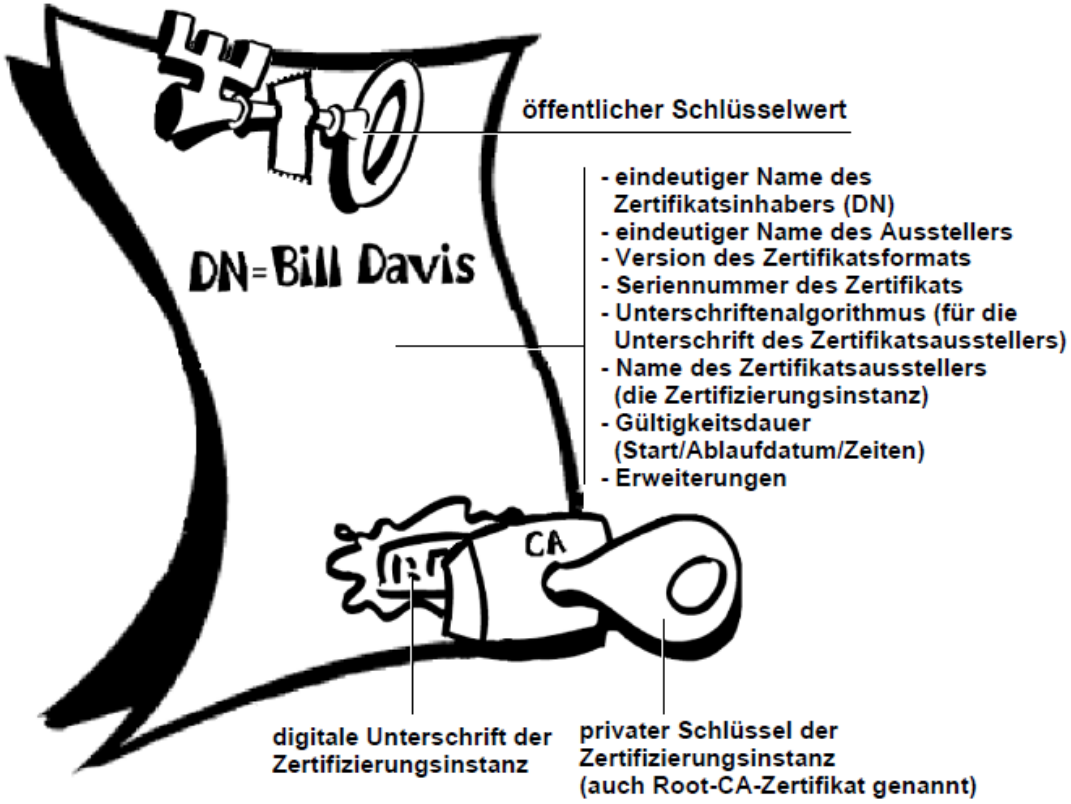
Bob-AG antwortet mit

Bob-AG BGF

❷ Alice verschlüsselt die Kartennummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG

Mr. X entschlüsselt zu **ACHTEINS**

Zertifikate und Trustcenter



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

Asymmetrische Verfahren

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

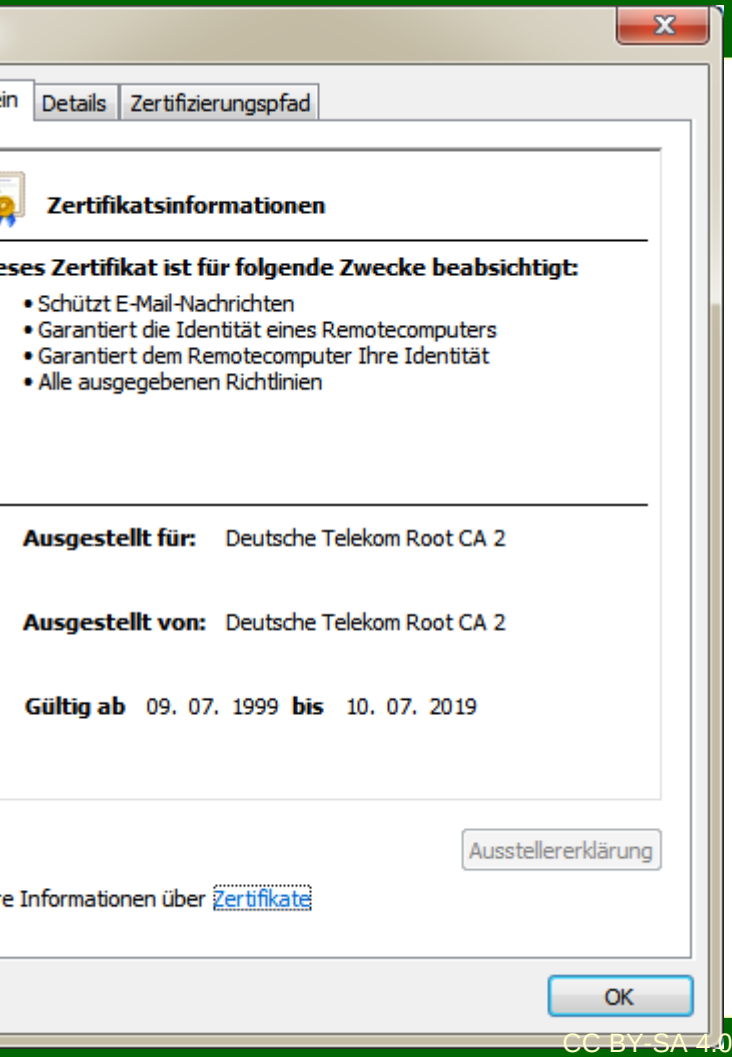
→ TC entschlüsselt zu **BOB-AG** und antwortet mit der signierten Information

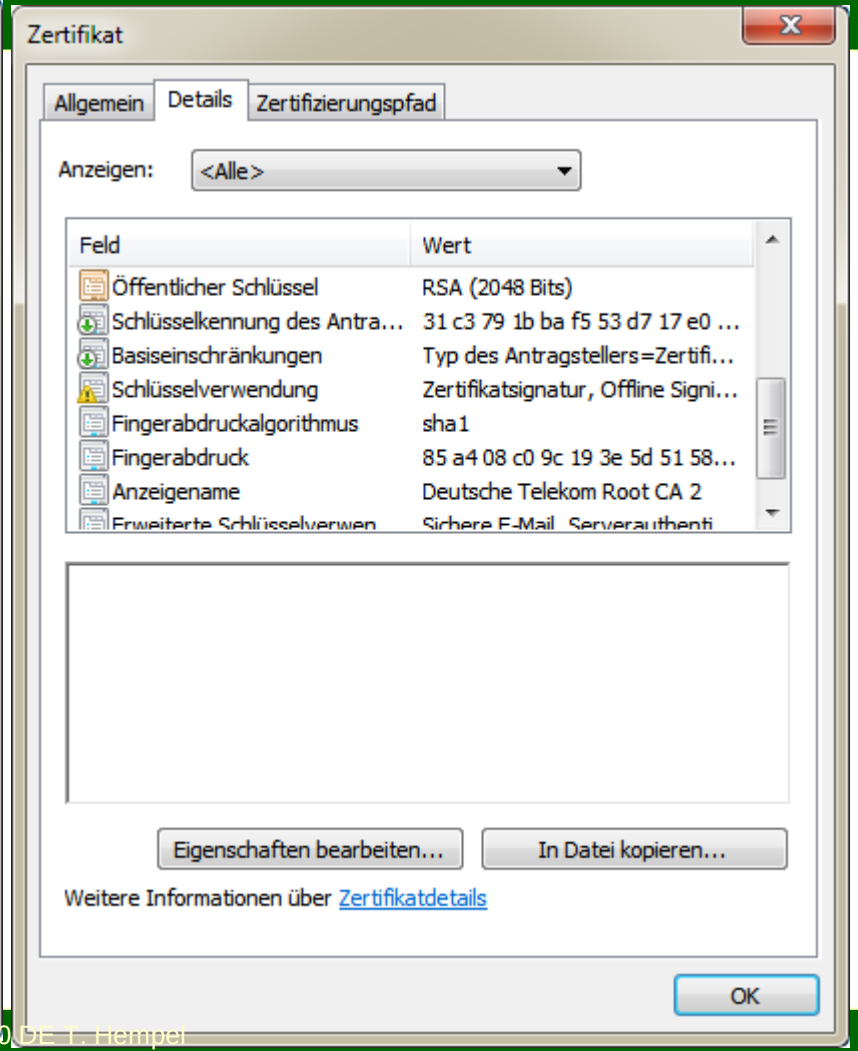
← **BOB-AG.BGF JMGKKFCGEH**

❷ Alice prüft die Signatur und erhält

BOB-AG.BGF BOB-AG.BGF

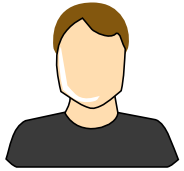
Zertifikat





Ausblick

Alice

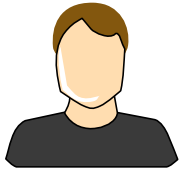


Bob-AG

```
+: BGF
-: FDB
```

Alice

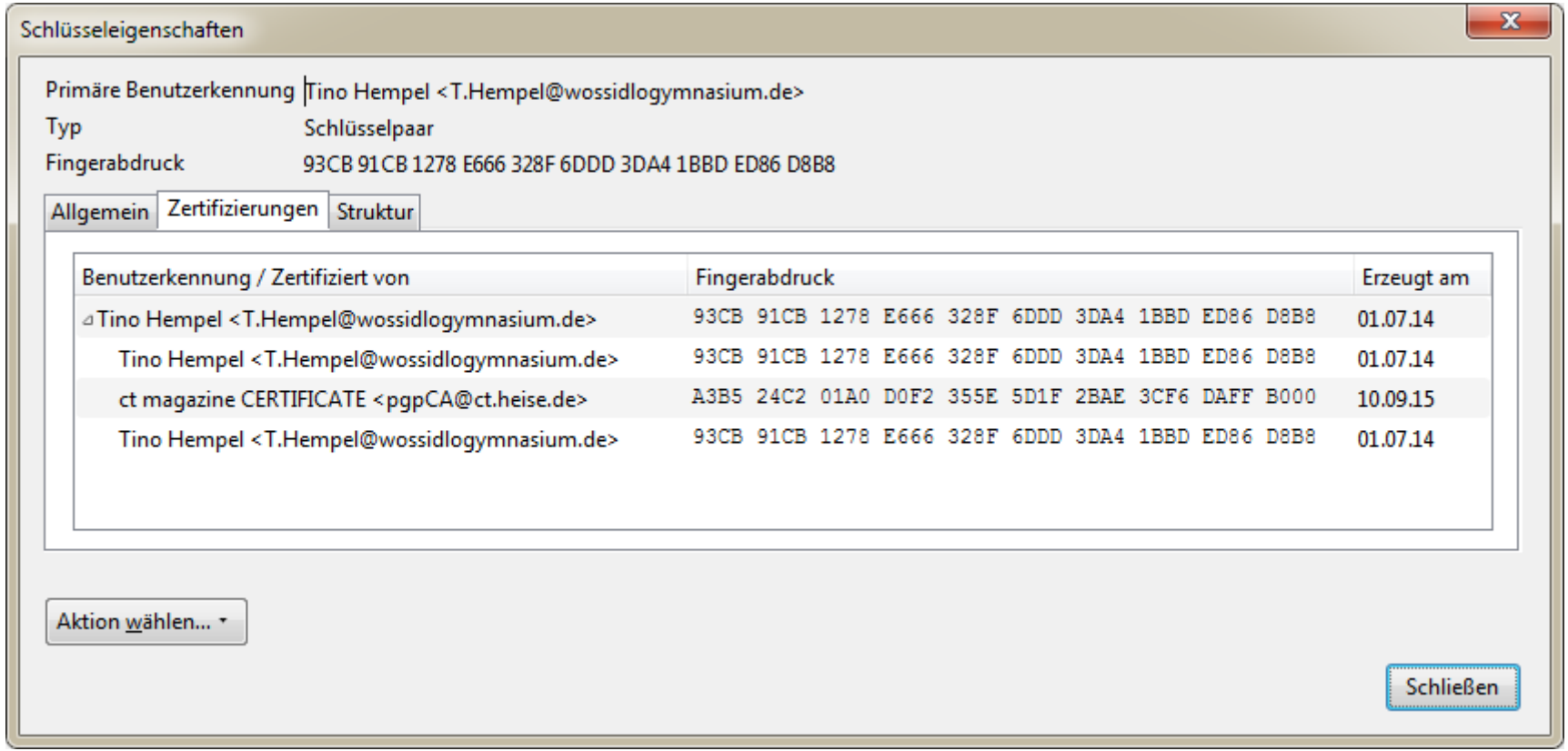
```
+: IKU
-: JUK
```



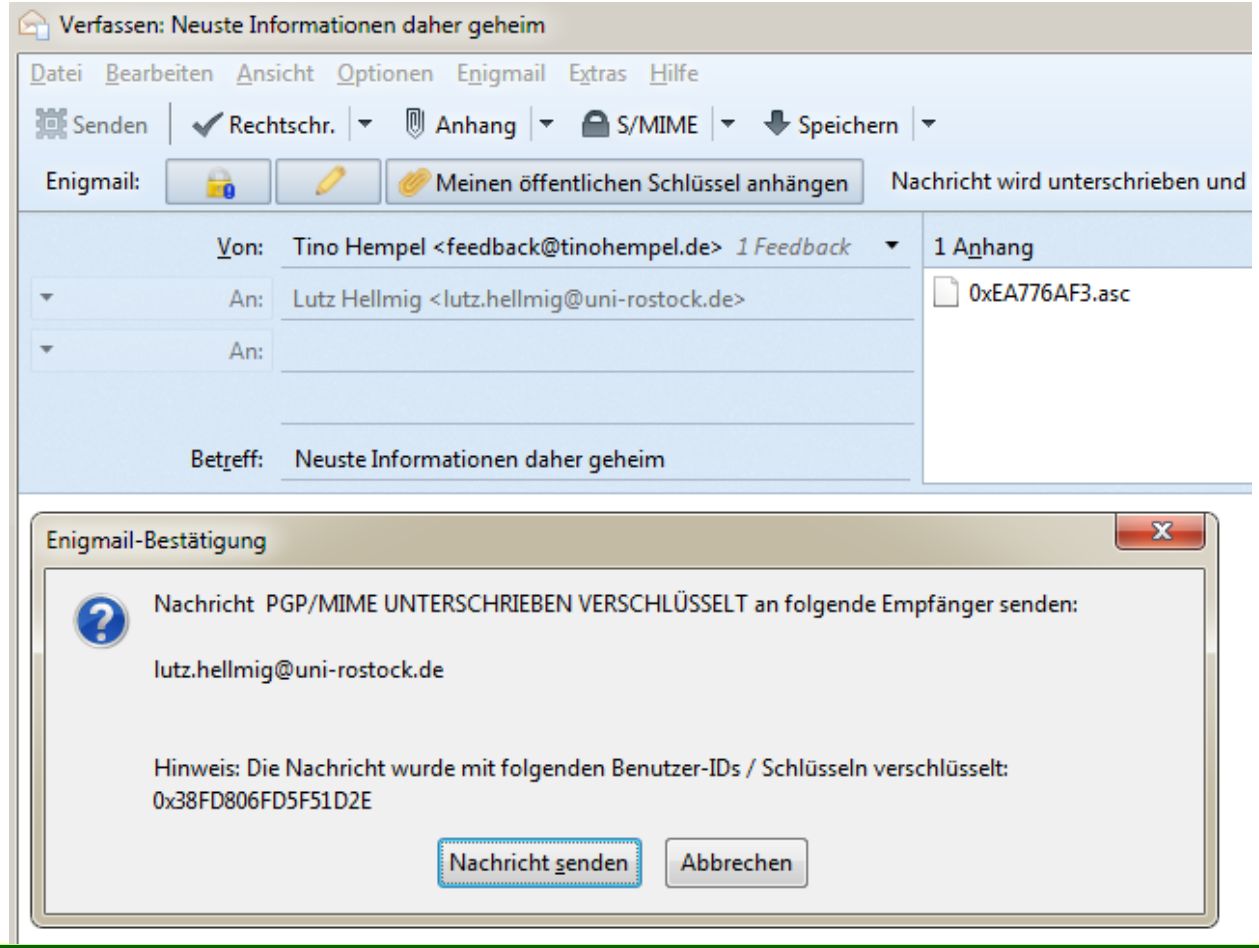
Bob-AG

```
+: BGF
-: FDB
```

E-Mail-Verschlüsselung



E-Mail-Verschlüsselung



Anregungen

- Inf-Schule:
  https://www.inf-schule.de/kommunikation/kryptologie
- Sicherheit macht Schule:
  https://www.sicherheit-macht-schule.de/
- Verfahrensübersicht
  http://kryptografie.de/kryptografie/index.htm
- Krypto im Advent:
  https://www.krypto-im-advent.de/