11/12.F2 Sichere Kommunikation

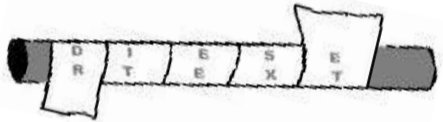
Historische Verfahren

Steganographie
verstecken

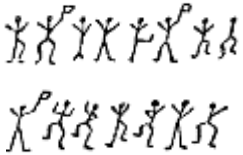
Kryptografie
verschlüsseln

Substitution
Zeichen/Wörter ersetzen

Transposition
Zeichen/Wörter umsortieren



Monoalphabetisch
Sherlock Holmes, Caesar

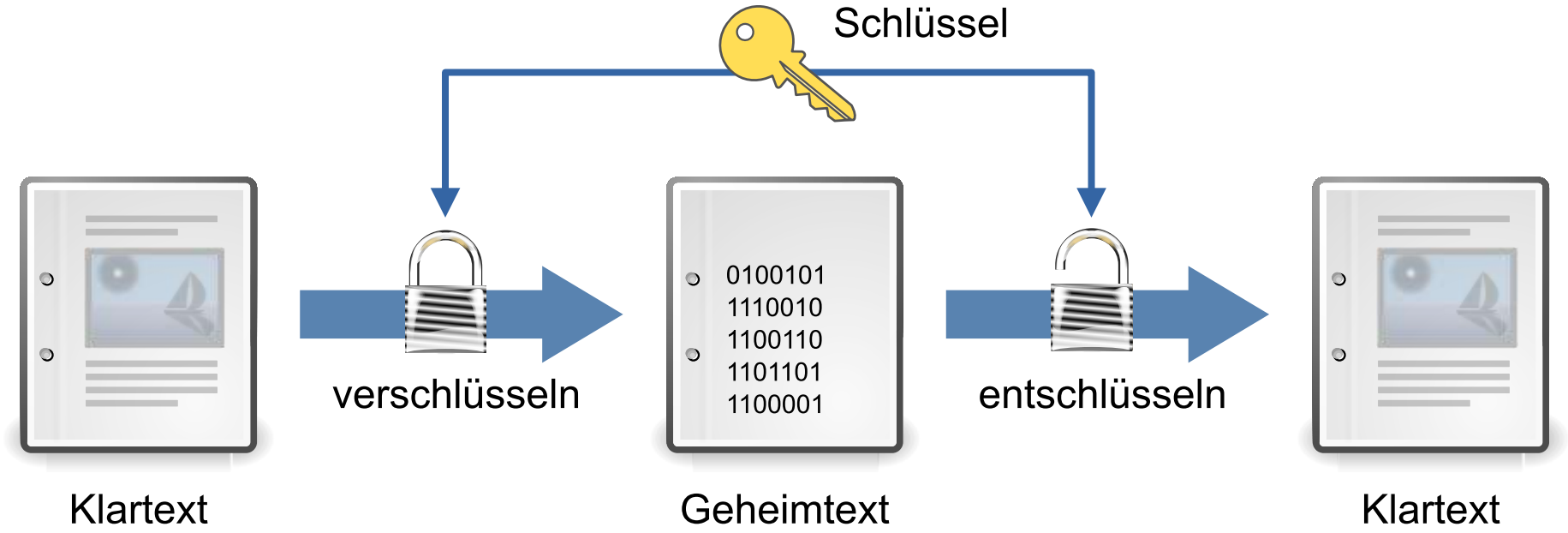


Polyalphabetisch
Vigenère, Enigma

One Time Pad

nach Witten, 2003

Verfahren



Sicherheitsziele

Vertraulichkeit

kein Mitlesen durch Fremde

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.

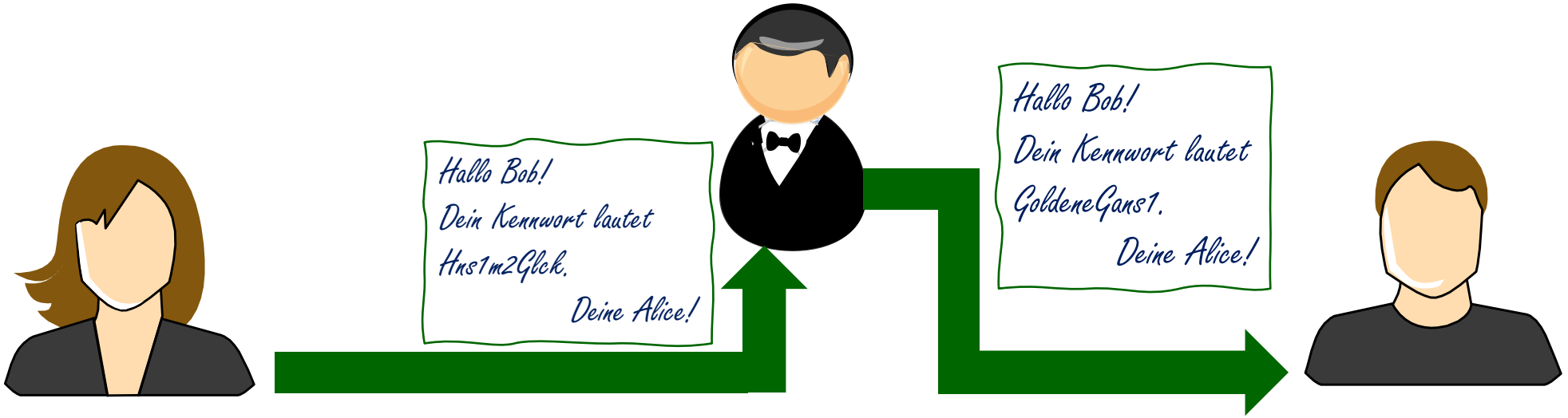
Benutzername *

Passwort *

Angemeldet bleiben

Anmelden

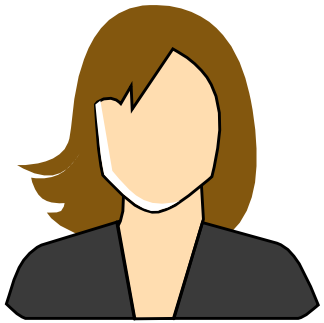
Sicherheitsziele



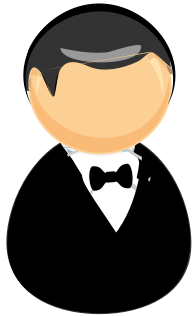
Integrität

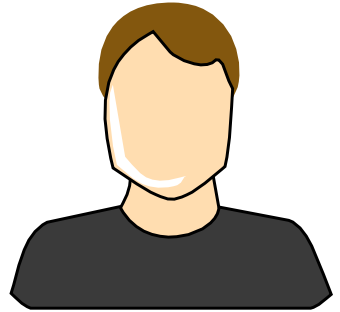
keine Manipulation durch Fremde

Sicherheitsziele



Alice





Bob

Authentizität

kein Fälschen des Absenders

Sicherheitsziele

Verbindlichkeit

kein Bestreiten der Urheberschaft

Serlo Informatik

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.

Kerkhoffs Prinzip

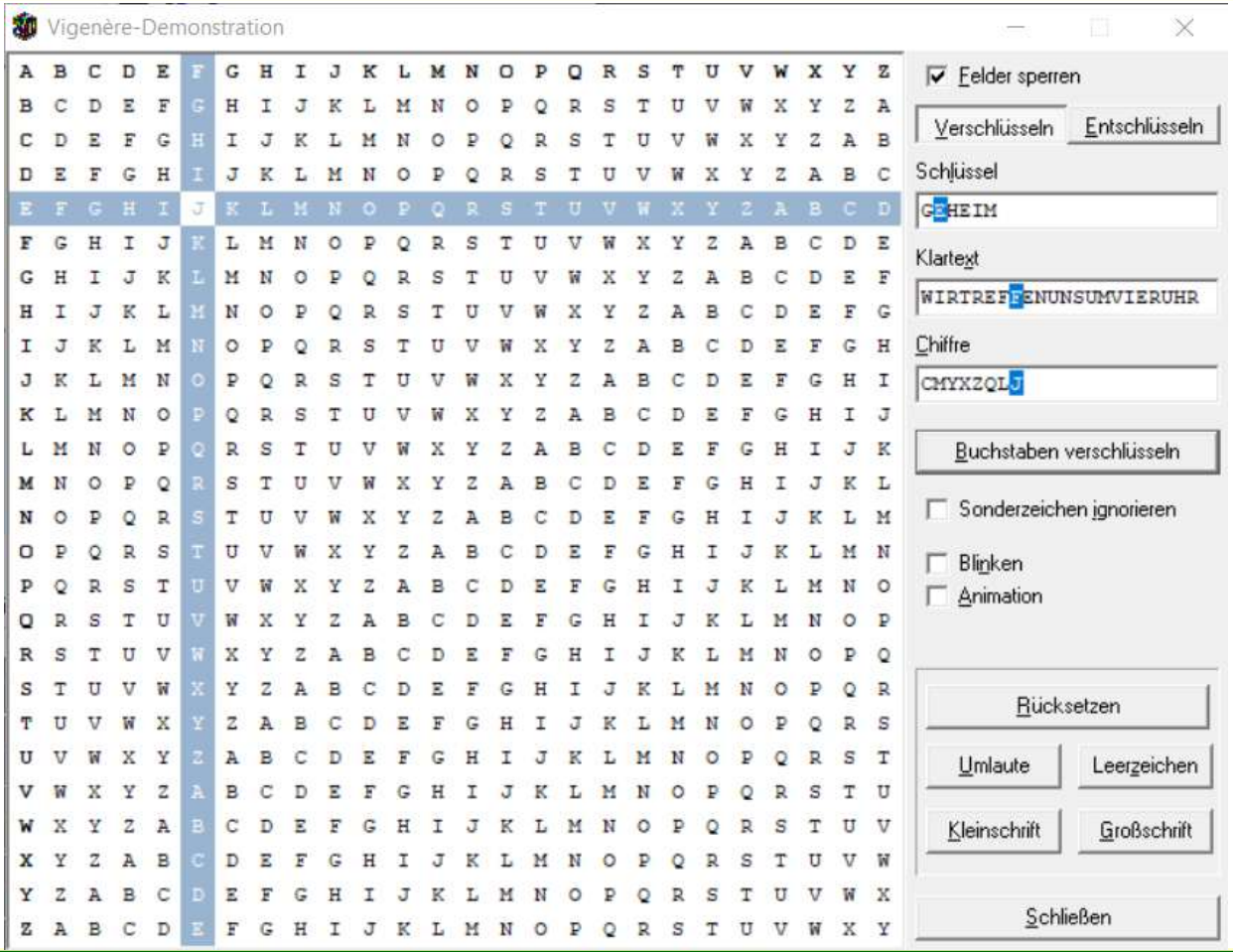
Das **Verfahren** muss im Wesentlichen unentzifferbar sein und darf keine Geheimhaltung erfordern.

Die **Schlüssel** bedürfen weiterhin der Geheimhaltung.

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

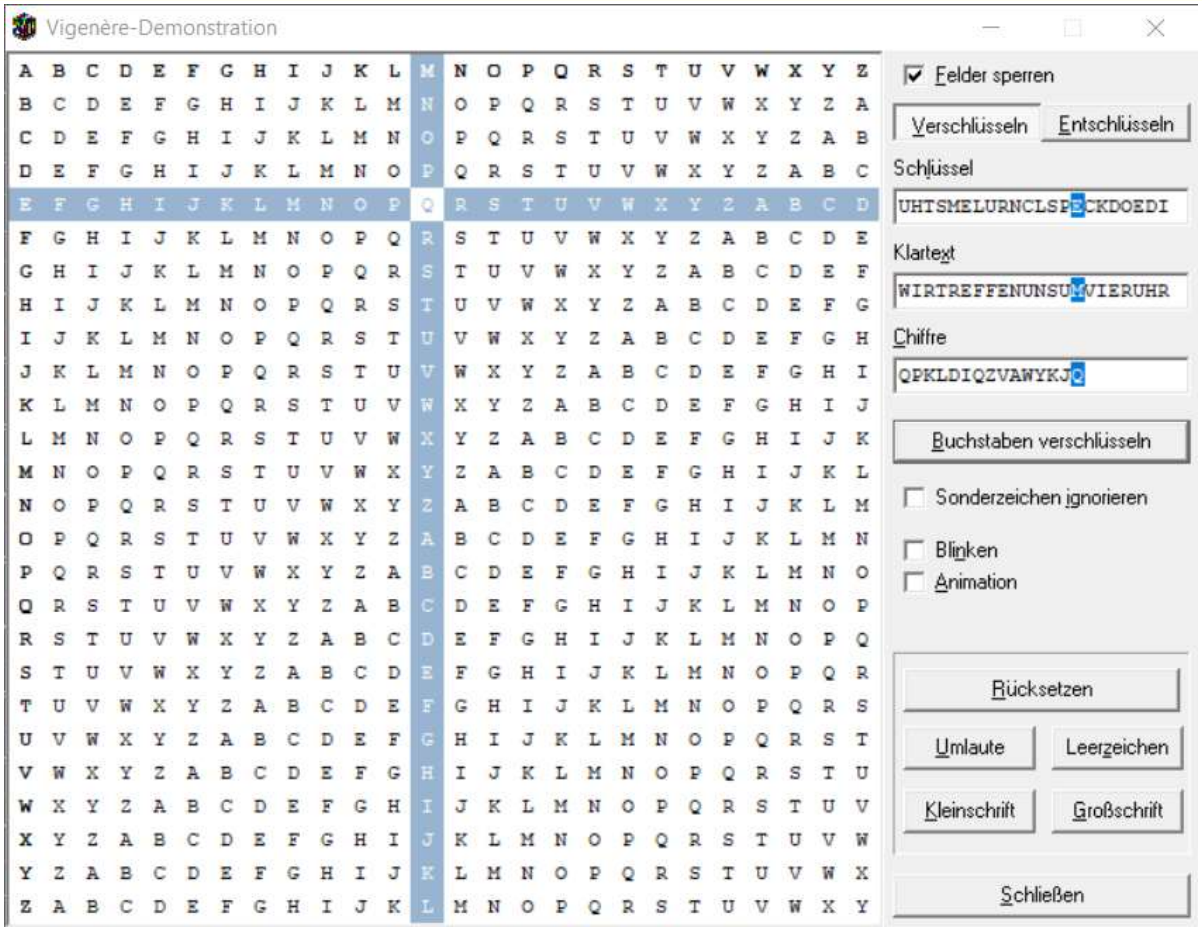
- Es ist schwieriger, ein kompromittiertes Verfahren zu ersetzen als einen kompromittierten Schlüssel.
- Es ist möglich, ein geheimes Verfahren durch Reverse Engineering zu rekonstruieren.
- Es ist leichter, Fehler/Hintertüren im Verfahren zu entdecken, wenn dieses öffentlich untersucht wird.
- Es ist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

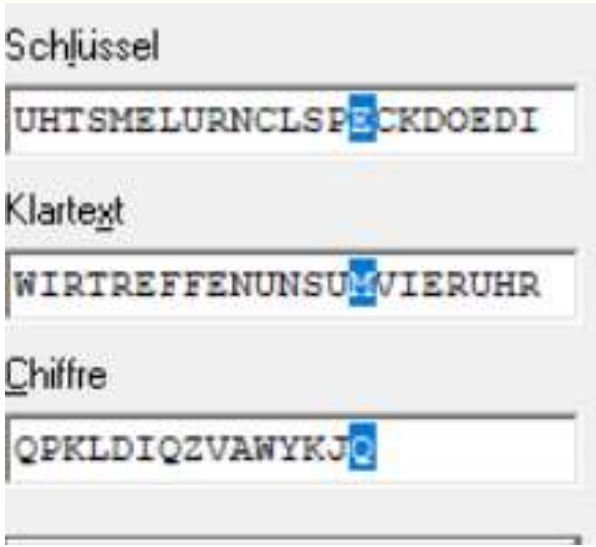
Vigenère-Verfahren



- polyalphabetisches Verfahren
- symmetrisches Verfahren

One-Time-Pad





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

One-Time-Pad

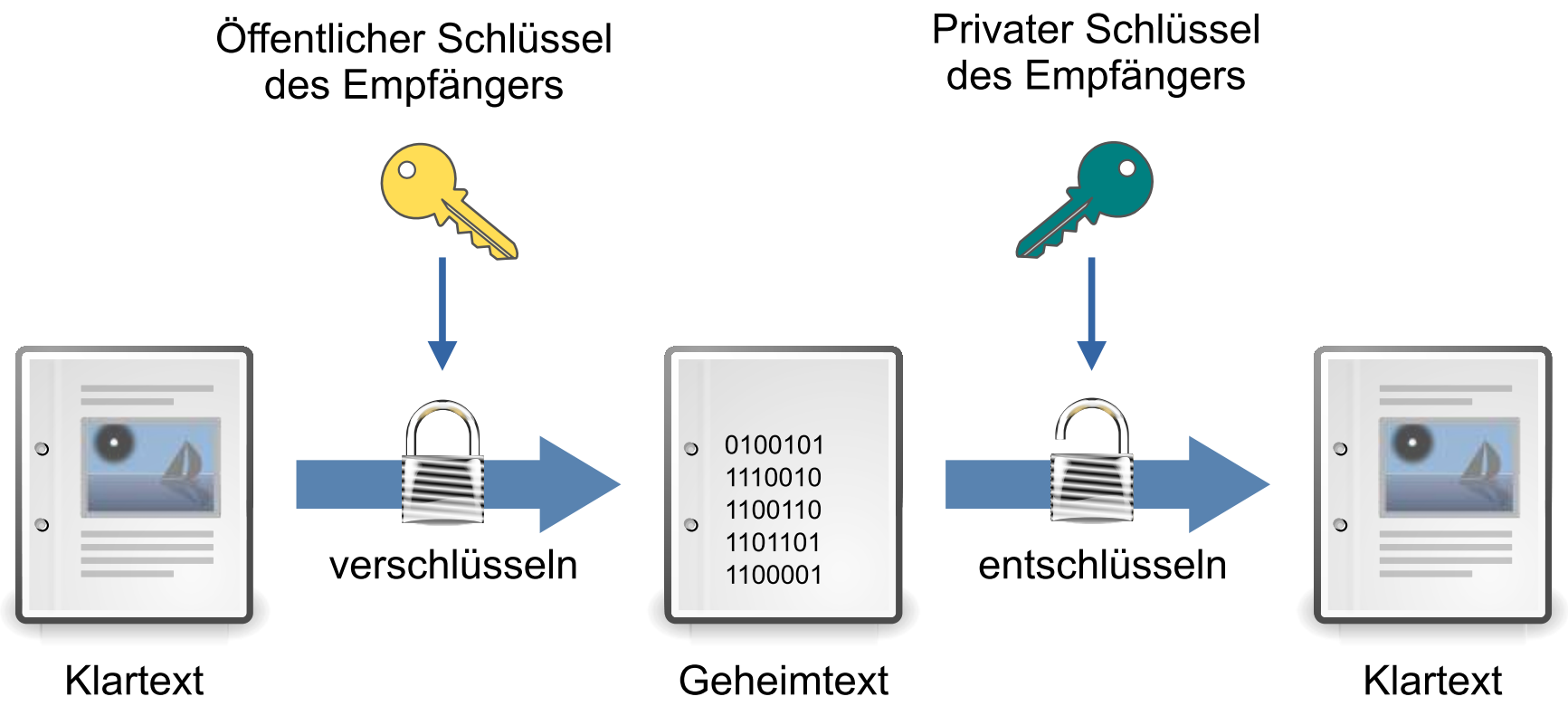
Aufgabe: Der Geheimtext MHOAYU wurde mit dem VIGENÈRE-Verfahren verschlüsselt.

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.

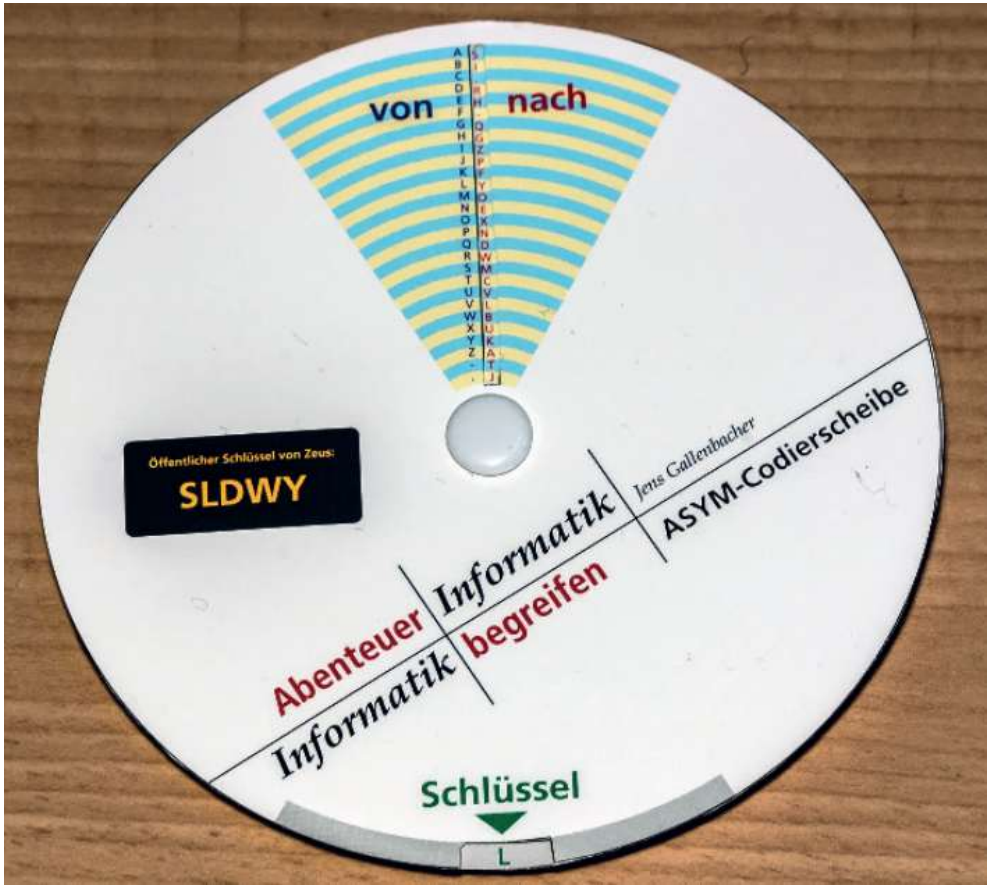
c) Leite eine Schlussfolgerung zur Sicherheit des VIGENÈRE-Verfahrens ab, wenn ein Schlüssel verwendet wird, der die gleiche Länge wie der Klartext hat.

Asymmetrische Verfahren



Asymmetrische Verfahren

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



Werkzeug ASYM-Kodierer

aus Gallenbacher. Abenteuer Informatik

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

aus Gallenbacher. Abenteuer Informatik

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

aus Gallenbacher. Abenteuer Informatik

Prüfe die Behauptung:

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

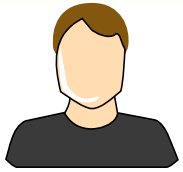
... und was passiert beim Schlüssel `PCT`?

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

Alice



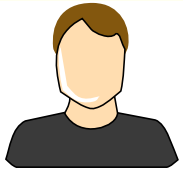
Bob-AG

```
ö: BGF
p: FDB
```

❶ Alice fragt Bob-AG nach deren public key

Asymmetrische Verfahren

Alice



Bob-AG

```
ö: BGF
p: FDB
```

❶ Alice fragt Bob-AG nach deren public key

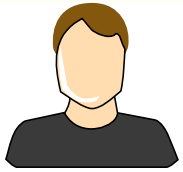
Bob-AG antwortet mit `BGF`

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: FDB

1. Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

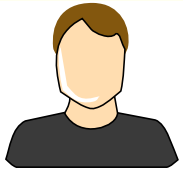
2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

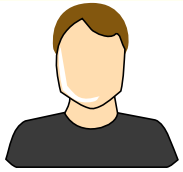
❷ Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key ⟶ ⟵ Bob-AG antwortet mit **BGF**

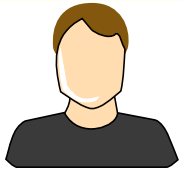
❷ Alice verschlüsselt die Kartennummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG ⟶ Bob-AG entschlüsselt:

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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

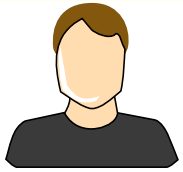
⟶ Bob-AG entschlüsselt: **ACHTEINS**

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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**

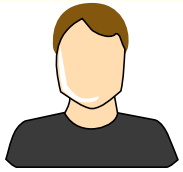
Bob-AG verschlüsselt **OK** mit private key zu

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key

⟶ Bob-AG antwortet mit **BGF**

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

⟶ Bob-AG entschlüsselt: **ACHTEINS**

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

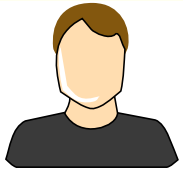
⟵ und sendet **OK** sowie das verschlüsselte **OK**

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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

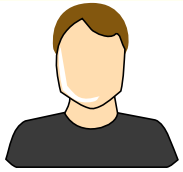
Bob-AG verschlüsselt **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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

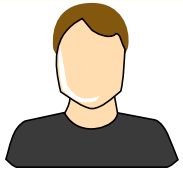
Bob-AG verschlüsselt **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**

Asymmetrische Verfahren

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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

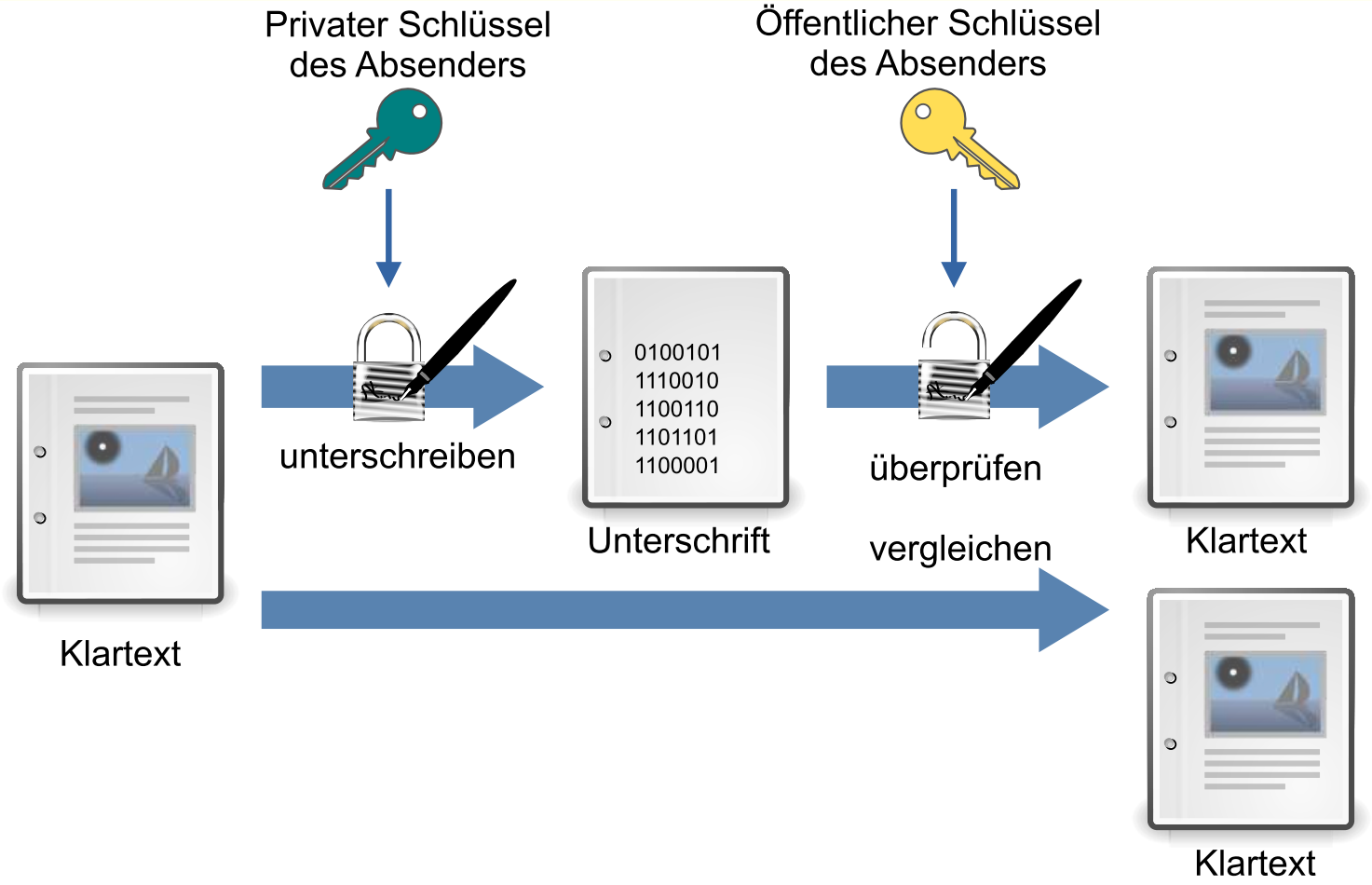
Bob-AG entschlüsselt: **ACHTEINS**

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

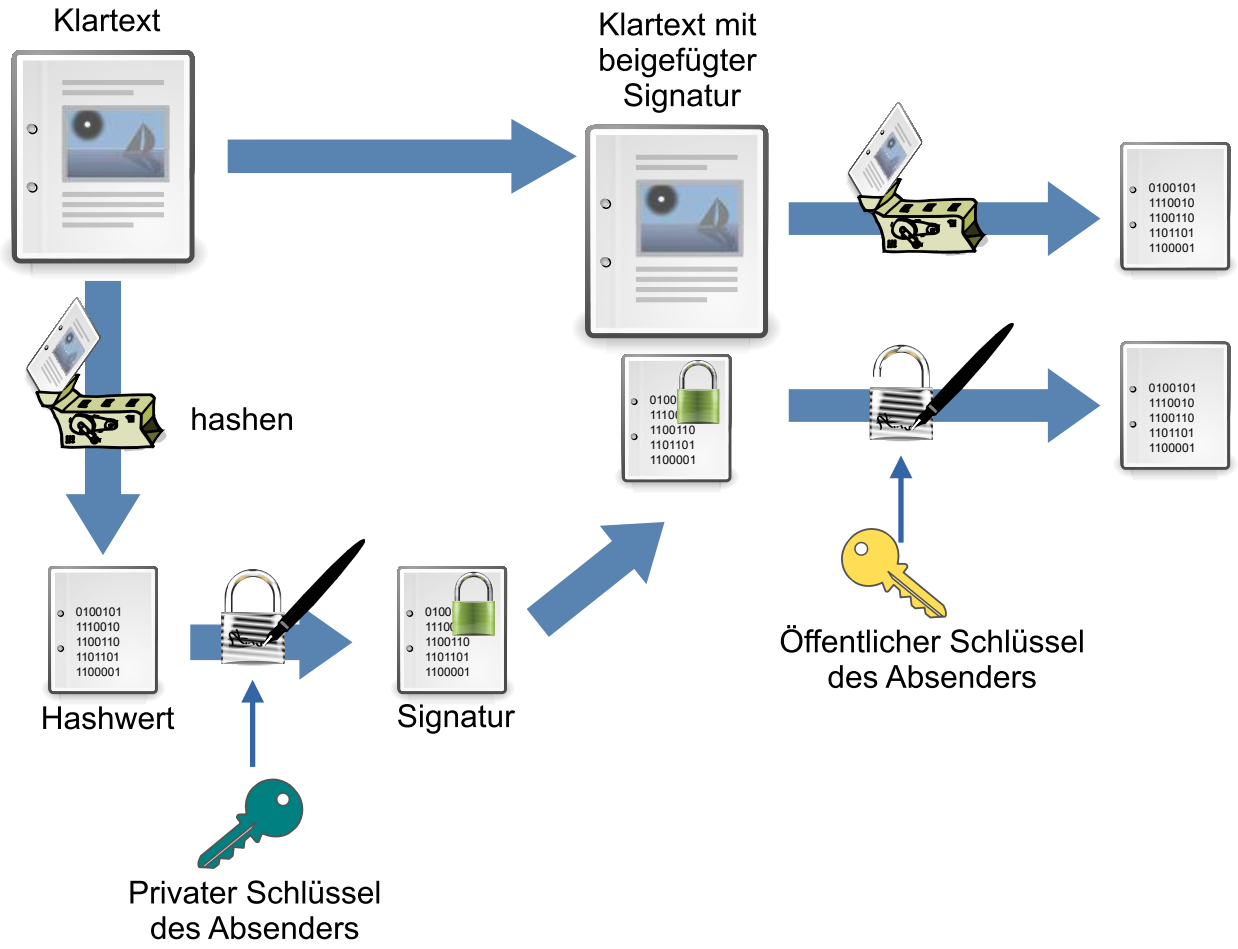
Bob-AG verschlüsselt **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**

Einwegfunktionen

Digitale Signatur



Digitale Signatur



Hashing

- **Kompression**
  Nachrichten beliebiger Länge werden auf Nachrichten einer festen Länge komprimiert.

- **Einwegfunktion**
  Aus dem Komprimat kann man nicht auf die Nachricht schlussfolgern.

- **Kollisionsresistenz**
  Es ist praktisch unmöglich, zwei verschiedene Nachrichten mit dem gleichen Hashwert zu finden.

Hashing

```
MD5-Hashwert der Datei: g07b_plane.jpg
hash1Byte Länge:16 Data:253DD04E87492E4FC3471DE5E776BC3D
MD5-Hashwert der Datei: g07b_ship.jpg
hash2Byte Länge:16 Data:253DD04E87492E4FC3471DE5E776BC3D
Die beiden MD5-Hashwerte sind gleich:true
```

Quelle: http://javacrypto.bplaced.net/g07-md5-hash-kollision/

Grenzen

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!**

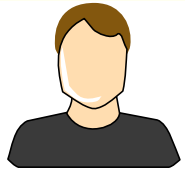
Quelle: https://www.martinstoeckli.ch/hash/de/index.php

Angriff

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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 **OK** mit private key zu **H.**
und sendet **OK** sowie das verschlüsselte **OK**

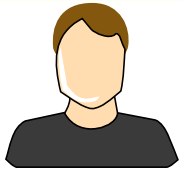
3. Alice erhält **OK H.**
und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis
OK = OK

Angriff

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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 **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**

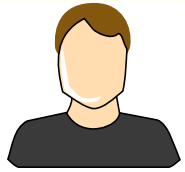
3. Alice erhält **OK H.** und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis **OK = OK**

Angriff

Alice

Bob-AG

BGF



Bob-AG

ö: BGF
p: 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

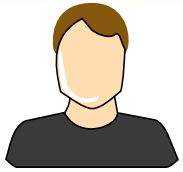
Bob-AG entschlüsselt: **ACHTEINS**

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

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

Angriff

Alice



Bob-AG

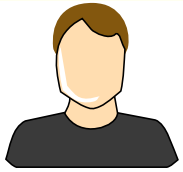
ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key

Angriff

Alice

ö: CEF
p: ZLB



Bob-AG

ö: BGF
p: FDB

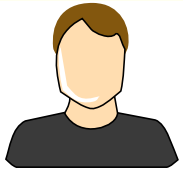
❶ Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit BGF

Angriff

Alice

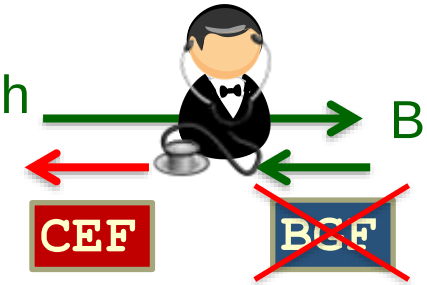
ö: CEF
p: ZLB



Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit BGF

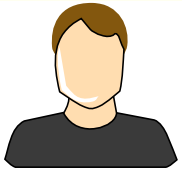
Angriff

Alice

Bob-AG

`CEF`

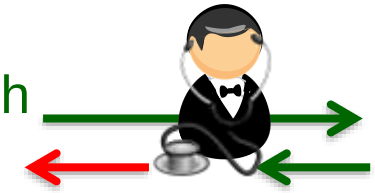
`ö: CEF`
`p: ZLB`



Bob-AG

`ö: BGF`
`p: FDB`

❶ Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit `BGF`

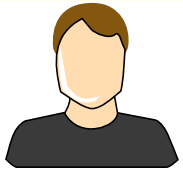
❷ Alice verschlüsselt die Kartennummer **`ACHTEINS`** zu

Angriff

Alice **CEF**

Bob-AG

ö: CEF
p: ZLB

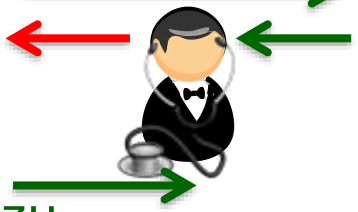


Bob-AG

ö: BGF
p: FDB

1. Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**



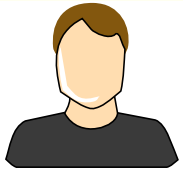
2. Alice verschlüsselt die Kartennummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG

Angriff

Alice **CEF**

Bob-AG

ö: CEF
p: ZLB



Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

Mr. X entschlüsselt zu

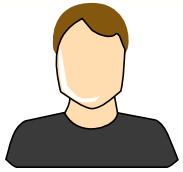
❷ Alice verschlüsselt die Kartennummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG

Angriff

Alice **CEF**

Bob-AG

ö: CEF
p: ZLB



Bob-AG

Bob-AG

ö: BGF
p: FDB

❶ Alice fragt Bob-AG nach deren public key

Bob-AG antwortet mit **BGF**

Mr. X entschlüsselt zu

ACHTEINS

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

Zertifikat

Öffentlicher Schlüssel
von Erna Mischke

Digitale Unterschrift
der Zertifizierungsstelle

Zertifikat

Alice `TC SLDWY`

`ö: CEF`
`p: ZLB`
`TC SLDWY`

TC: Trust Center

`ö: SLDWY`
`p: TEG-V`
`Bob-AG BGF`
`Mr. X CEF`

1. Alice verschlüsselt die Frage nach public key Bob-AG zu

Zertifikat

Alice **TC SLDWY**

ö: CEF
p: ZLB
TC SLDWY

TC: Trust Center

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

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

Zertifikat

Alice **TC SLDWY**

ö: CEF
p: ZLB
TC SLDWY

TC: Trust Center

ö: SLDWY
p: 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

Zertifikat

Alice `TC SLDWY`

`ö: CEF`
`p: ZLB`
`TC SLDWY`

TC: Trust Center

`ö: SLDWY`
`p: 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

Zertifikat

Alice `TC SLDWY`

`ö: CEF`
`p: ZLB`
`TC SLDWY`

TC: Trust Center

`ö: SLDWY`
`p: 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`

Zertifikat

Alice **TC SLDWY**

ö: CEF
p: ZLB
TC SLDWY

TC: Trust Center

ö: SLDWY
p: 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

Zertifikat

Alice **TC SLDWY**

ö: CEF
p: ZLB
TC SLDWY

TC: Trust Center

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

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

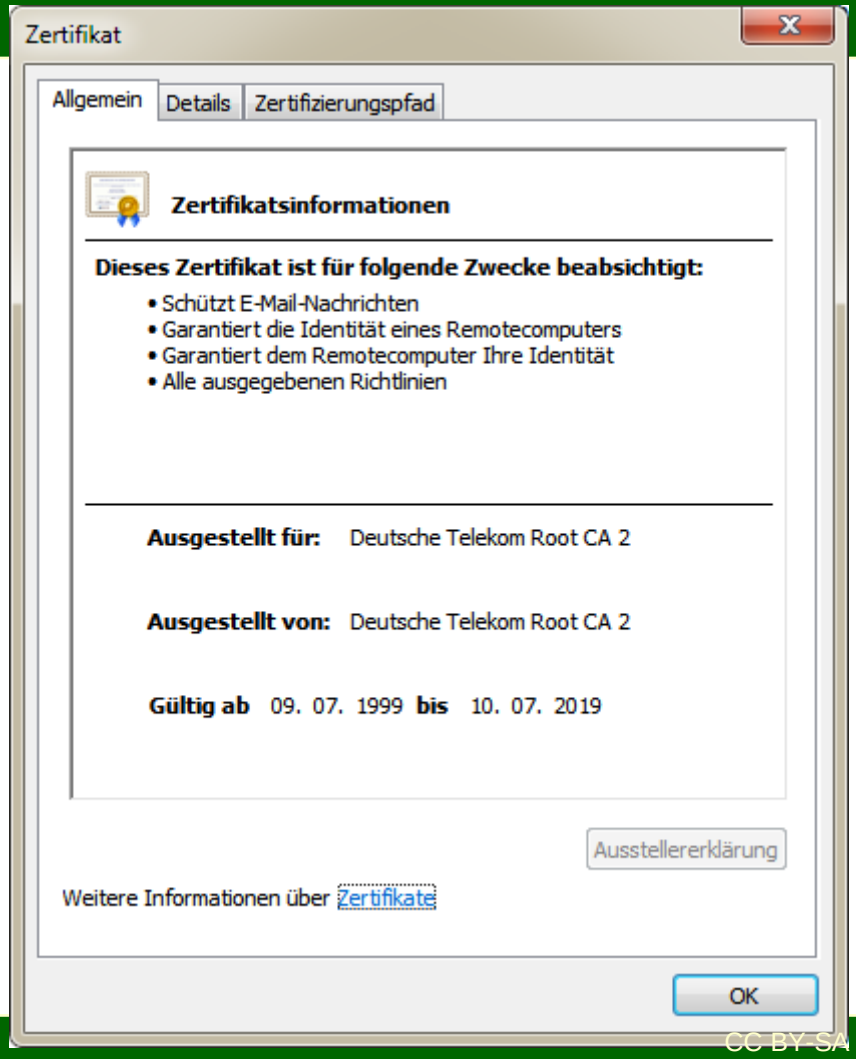
TC entschlüsselt zu **BOB-AG** und antwortet mit der signierten Information

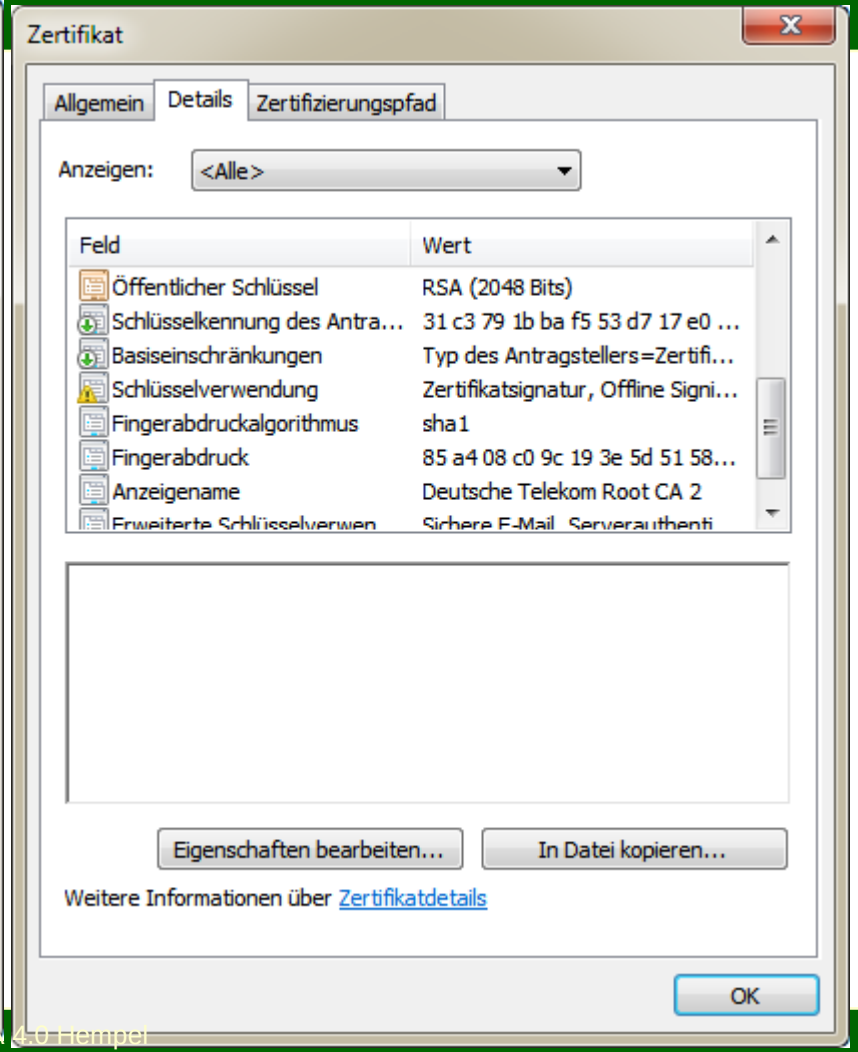
BOB-AG.BGF JMGKKFCGEH

2. Alice prüft die Signatur und erhält

BOB-AG.BGF BOB-AG.BGF

Zertifikat





Diffie-Hellman-Schlüsseltausch

Ein Pfund Gehacktes

Ausblick

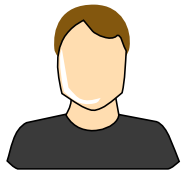
TC: Trust Center

ö: SLDWY
p: TEG-V
Bob-AG BGF
Mr. X CEF
Alice IKU

ö: CEF
p: ZLB
TC SLDWY

Alice

TC SLDWY
ö: IKU
p: JUK



Bob-AG

TC SLDWY
ö: BGF
p: FDB