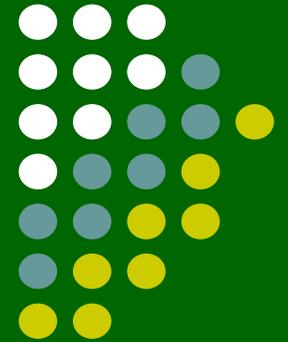


11/12.F2 Sichere Kommunikation





Historische Verfahren



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.

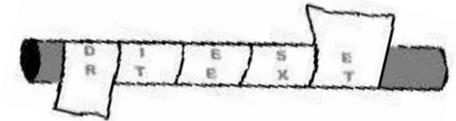
Kryptografie verschlüsseln

Substitution

Zeichen/Wörter ersetzen

Transposition

Zeichen/Wörter umsortieren



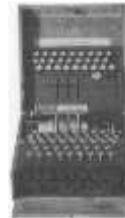
Monoalphabetisch

Sherlock Holmes, Caesar



Polyalphabetisch

Vigenère, Enigma

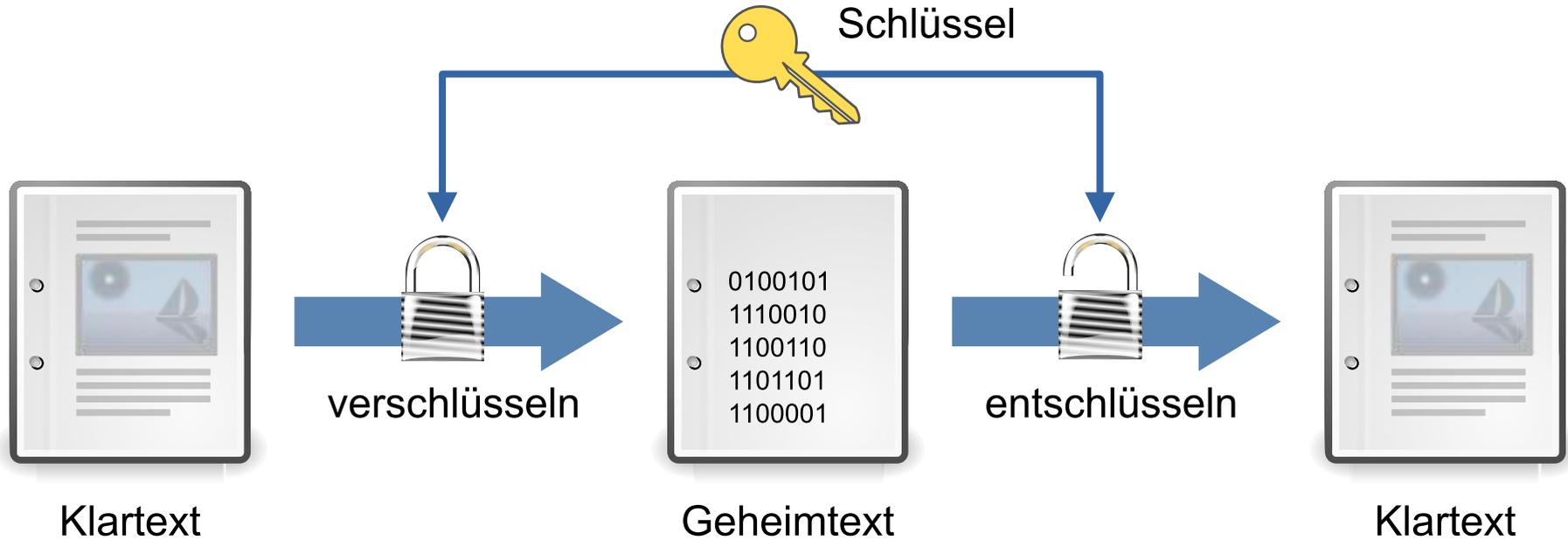


One Time Pad



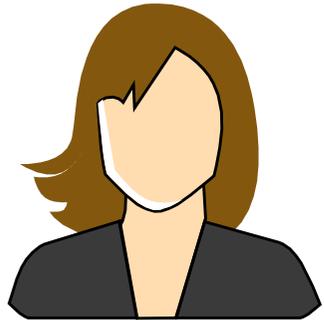


Verfahren



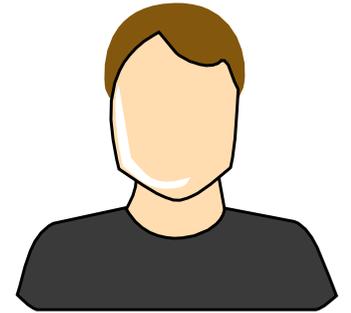


Sicherheitsziele



Alice

Hallo Bob!
Dein Kennwort lautet
Hns1m2Glek.
Deine Alice!



Bob

Vertraulichkeit
kein Mitlesen durch Fremde



Interner Bereich



Nicht sicher | löwenzahn-schule.de/impresum/interner-bereich



LÖWENZAHN SCHULE

[Startseite](#)

[Schule](#)

[Termine](#)

[Förderverein](#)

[Kontakt](#)

[Impresum/Datenschutz](#)

Interner Bereich

Die Anmeldung ist für die Redakteure der Homepage vorgesehen.

Benutzername *

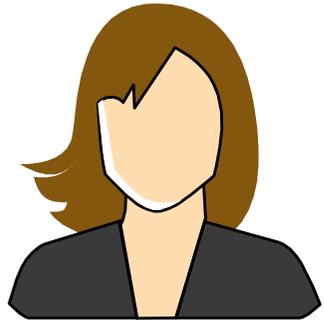
Passwort *

Angemeldet bleiben

Anmelden

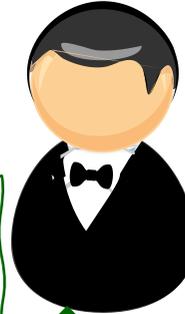


Sicherheitsziele

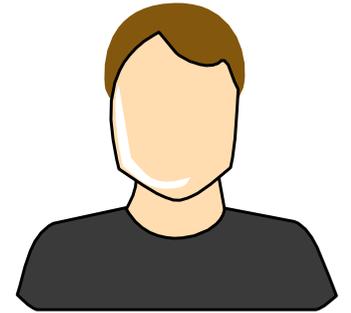


Alice

Hallo Bob!
Dein Kennwort lautet
Hns1m2Glek.
Deine Alice!



Hallo Bob!
Dein Kennwort lautet
GoldeneGans1.
Deine Alice!



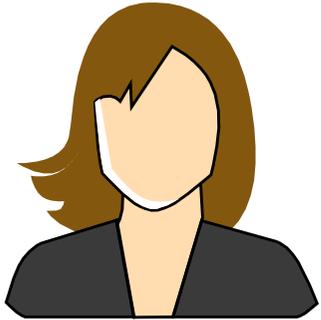
Bob

Integrität

keine Manipulation durch Fremde



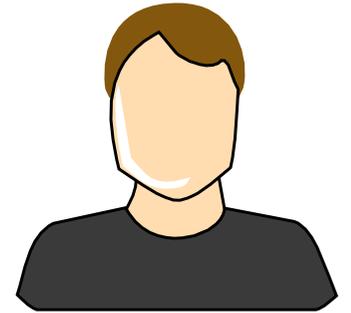
Sicherheitsziele



Alice



Hallo Bob!
Dein Kennwort lautet
GoldeneGans1.
Deine Alice!



Bob

Authentizität

kein Fälschen des Absenders:



Sicherheitsziele



Alice

Verbindlichkeit

Bob

kein Bestreiten der Urheberschaft



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.

Dieses Werk steht unter der freien Lizenz [cc-by-sa-4.0](#) Information



Kerkhoffs Prinzip



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 Drexler, Historico de la Mondo Lingvo (Leipzig, 1931), 102



Vigenère-Verfahren



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
WIRTSCHAFTSRECHENUNGSANLEHNER

Chiffre
CMYXZQL

Buchstaben verschlüsseln

Sonderzeichen ignorieren

Blinken

Animation

Rücksetzen

Umlaute Leerzeichen

Kleinschrift Großschrift

Schließen

- polyalphabetisches Verfahren
- symmetrisches Verfahren



One-Time-Pad



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
UHTSMELURNCLSP**E**CKDOEDI

Klartext
WIRTREFFENUN**S**UMVIERUHR

Chiffre
QP**K**LDIQZVAVYK**J**Q

Buchstaben verschlüsseln

Sonderzeichen ignorieren

Blinken

Animation

Rücksetzen

Umlaute Leerzeichen

Kleinschrift Großschrift

Schließen

Schlüssel
UHTSMELURNCLSP**E**CKDOEDI

Klartext
WIRTREFFENUN**S**UMVIERUHR

Chiffre
QP**K**LDIQZVAVYK**J**Q

- 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.



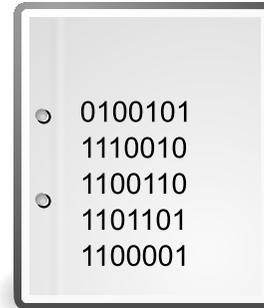
Asymmetrische Verfahren



Öffentlicher Schlüssel
des Empfängers



verschlüsseln



Geheimtext

Privater Schlüssel
des Empfängers



entschlüsseln



Klartext



Klartext



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

1 Alice fragt Bob-AG nach deren public key





Asymmetrische Verfahren



Alice



Bob-AG

ö : BGF
p : FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit **BGF**

BGF



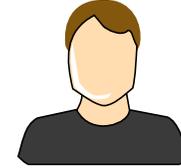
Asymmetrische Verfahren



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 Kartenummer **ACHTEINS** zu



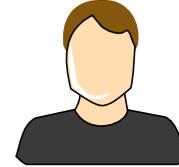
Asymmetrische Verfahren



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 Kartenummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG





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 Kartenummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG



Bob-AG entschlüsselt:



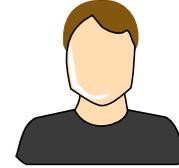
Asymmetrische Verfahren



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 Kartenummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG



Bob-AG entschlüsselt: **ACHTEINS**

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



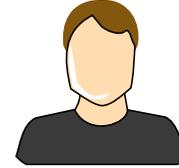
Asymmetrische Verfahren



Alice

Bob-AG

BGF



Bob-AG

ö : BGF

p : FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit BGF

2 Alice verschlüsselt die Kartenummer **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**



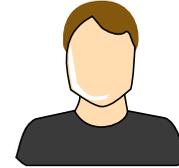
Asymmetrische Verfahren



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 Kartenummer **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 Kartenummer **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**



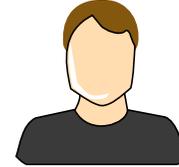
Asymmetrische Verfahren



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 Kartenummer **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**

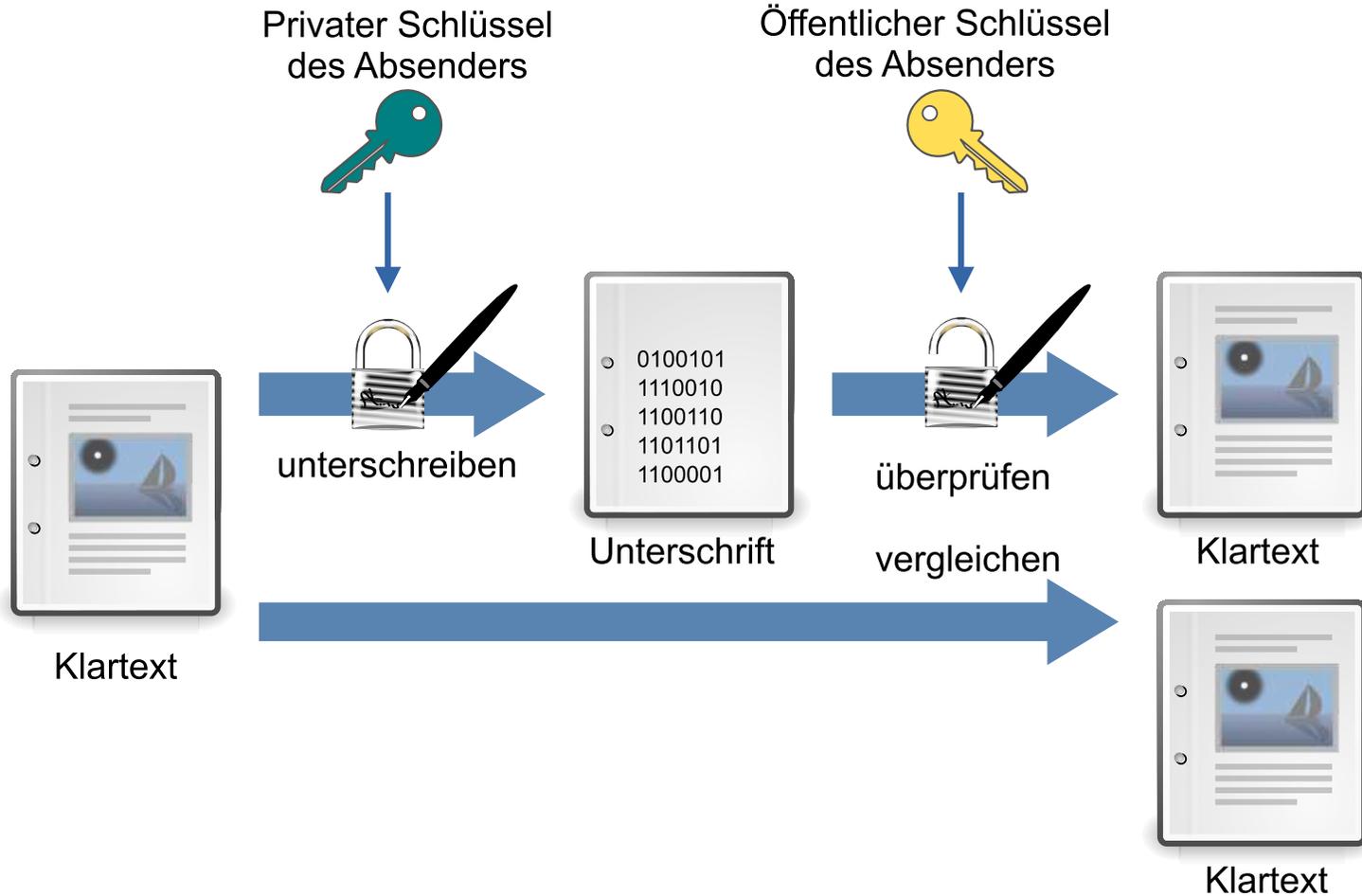


Einwegfunktionen



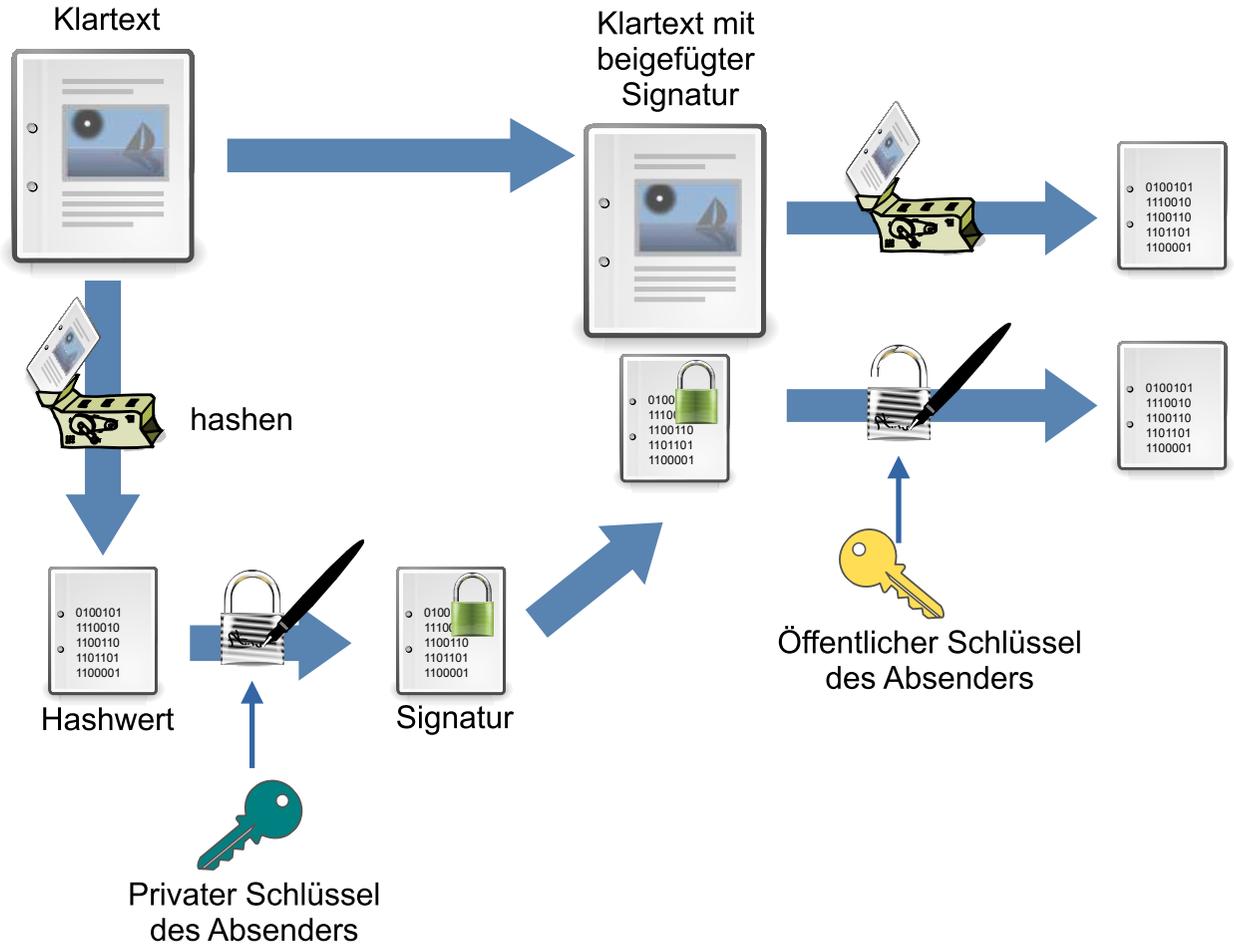


Digitale Signatur





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 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 ~ 50 Giga MD5 Werte pro Sekunde (Stand 2021), um unsere Beispiel Rainbow-table zu erstellen braucht man also nur **0.4 Sekunden!**



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 Kartenummer **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

BGF



Bob-AG

ö : BGF

p : FDB

- 1 Alice fragt Bob-AG nach deren public key
- 2 Alice verschlüsselt die Kartenummer **ACHTEINS** zu **TYLWC.SW** und sendet an Bob-AG
- 3 Alice erhält **OK H.** und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis **OK = OK**



Bob-AG antwortet mit **BGF**

Bob-AG entschlüsselt: **ACHTEINS**

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

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



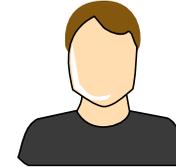
Angriff



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 Kartenummer **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**

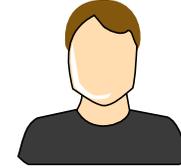


Angriff



Alice

ö : CEF
p : ZLB



Bob-AG

ö : BGF
p : FDB

1 Alice fragt Bob-AG nach deren public key



Angriff



Alice

ö: CEF
p: ZLB



Bob-AG

ö: BGF
p: FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit **BGF**

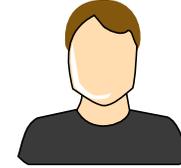


Angriff



Alice

ö: CEF
p: ZLB



Bob-AG

ö: BGF
p: FDB

1 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

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit **BGF**

2 Alice verschlüsselt die Kartenummer **ACHTEINS** zu

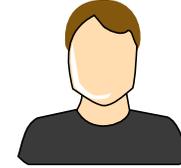


Angriff



Alice Bob-AG
ö: CEF
p: ZLB

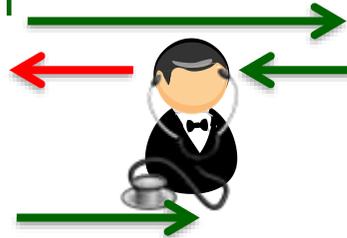
ö: CEF
p: ZLB



Bob-AG ö: BGF
p: FDB

ö: BGF
p: FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit BGF

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

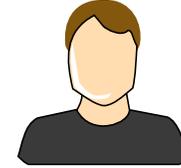


Angriff



Alice Bob-AG
CEF

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 Kartenummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG

Mr. X entschlüsselt zu

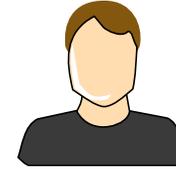


Angriff



Alice Bob-AG
CEF

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 Kartenummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG

Mr. X entschlüsselt zu
ACHTEINS



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



1 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



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



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



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

2 Alice prüft die Signatur und erhält

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

2 Alice prüft die Signatur und erhält

BOB-AG.BGF JMGKKFCGEH

BOB-AG.BGF BOB-AG.BGF



Zertifikat



Zertifikat

Allgemein Details Zertifizierungspfad

Zertifikatsinformationen

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Schützt E-Mail-Nachrichten
- Garantiert die Identität eines Remotecomputers
- Garantiert dem Remotecomputer Ihre Identität
- Alle ausgegebenen Richtlinien

Ausgestellt für: Deutsche Telekom Root CA 2

Ausgestellt von: Deutsche Telekom Root CA 2

Gültig ab 09. 07. 1999 **bis** 10. 07. 2019

[Ausstellererklärung](#)

Weitere Informationen über [Zertifikate](#)

OK

Zertifikat

Allgemein Details Zertifizierungspfad

Anzeigen: <Alle>

Feld	Wert
Öffentlicher Schlüssel	RSA (2048 Bits)
Schlüsselkennung des Antra...	31 c3 79 1b ba f5 53 d7 17 e0 ...
Basiseinschränkungen	Typ des Antragstellers=Zertifi...
Schlüsselverwendung	Zertifikatsignatur, Offline Signi...
Fingerabdruckalgorithmus	sha1
Fingerabdruck	85 a4 08 c0 9c 19 3e 5d 51 58...
Anzeigename	Deutsche Telekom Root CA 2
Erweiterte Schlüsselverwen	Sichere E-Mail Serverauthent...

[Eigenschaften bearbeiten...](#) [In Datei kopieren...](#)

Weitere Informationen über [Zertifikatdetails](#)

OK



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



TC SLDWY

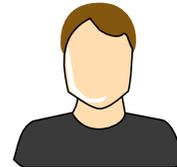
ö: IKU
p: JUK



Alice

TC SLDWY

ö: BGF
p: FDB



Bob-AG