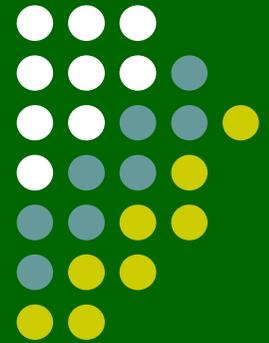


Sicher kommunizieren

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
<p>mithilfe eines Internetdienstes kommunizieren</p> <ul style="list-style-type: none">• Nachrichten unter Angabe eines geeigneten Betreffs an einen oder mehrere Empfänger versenden• Anhänge hinzufügen und speichern• Authentizität und Gefahrenpotential von eingehenden Nachrichten abschätzen• mit personenbezogenen Daten verantwortungsbewusst umgehen	<p>Ein geeigneter Dienst ist die E-Mail. Neuerstellung, Beantwortung und Weiterleitung sind Möglichkeiten des Versendens von Nachrichten.</p> <p>Die Schülerinnen und Schüler können die Dateigröße in der Maßeinheit Byte mit Präfixen und den Dateityp angeben.</p> <p>Die Beurteilung erfolgt anhand der Absenderadresse, des Betreffs oder des Inhalts. Die Schülerinnen und Schüler reagieren in geeigneter Weise.</p> <p>Die Schülerinnen und Schüler beachten sowohl den Schutz der eigenen Daten als auch den</p>



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
<p>Verschlüsselung verstehen</p> <ul style="list-style-type: none">• klassische Verfahren der symmetrischen Verschlüsselung anschaulich erläutern• kurze Nachrichten verschlüsselt austauschen <p>Vertraulichkeit herstellen</p>	<p>Verschlüsselung ist eine Codierung, bei der die Decodierung für Außenstehende nicht möglich sein soll.</p> <p>Die Schülerinnen und Schüler beschreiben klassische Verfahren unter Verwendung der Begriffe Klartext- und Geheimentextalphabet, Klartext und Geheimentext, Schlüssel, Verschlüsseln und Entschlüsseln. Sie erkennen, dass durch Verschlüsselung eine vertrauliche Kommunikation ermöglicht wird.</p> <p>Die Schülerinnen und Schüler argumentieren zur Sicherheit der Verfahren.</p>



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 <ul style="list-style-type: none">Prinzip der asymmetrischen Verschlüsselung	Die Prinzipien sind anschaulich und enaktiv-haptisch zu vermitteln. Die asymmetrische Verschlüsselung wird zur Sicherung der Vertraulichkeit, Authentizität und Integrität eingesetzt.
Codierung verstehen <ul style="list-style-type: none">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
[MD] [BO] [BNE] [DRF] [PG]

ca. 20 Unterrichtsstunden

ca. 12 Unterrichtsstunden

Verbindliche Ziele und Inhalte	Hinweise und Anregungen
<ul style="list-style-type: none">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

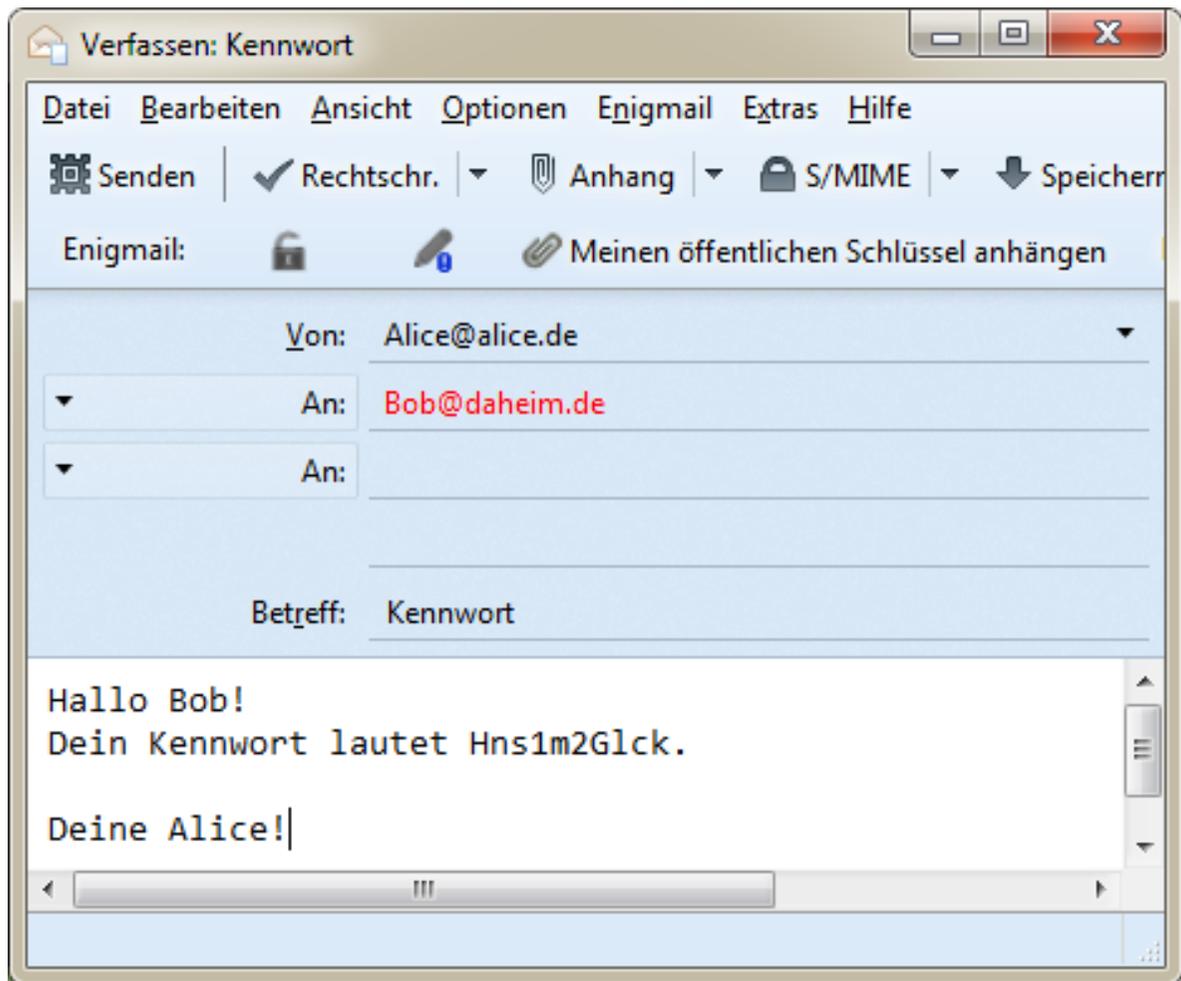


Hallo Bob!
Dein Kennwort lautet
Hns1m2Glck.

Deine Alice!



Hallo Bob!
Das Kennwort lautet
Hns1m2Glck.



*Drahtlosnetzwerkverbindung

File Edit View Navigation Record Analyze Statistics Telephony Wireless Tools Help

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



[Startseite](#)

[Schule](#)

[Termine](#)

[Förderverein](#)

[Kontakt](#)

[Impresum/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

Sicher Kommunizieren Einfach Erklärt - 5/5

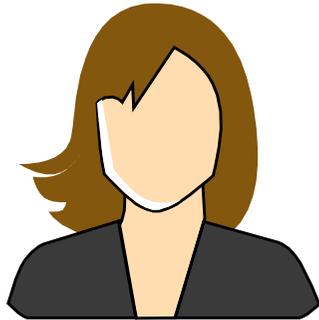


Das letzte von fünf Videos von Alexander Lehmann zum Thema Verschlüsselung und Datenschutz.

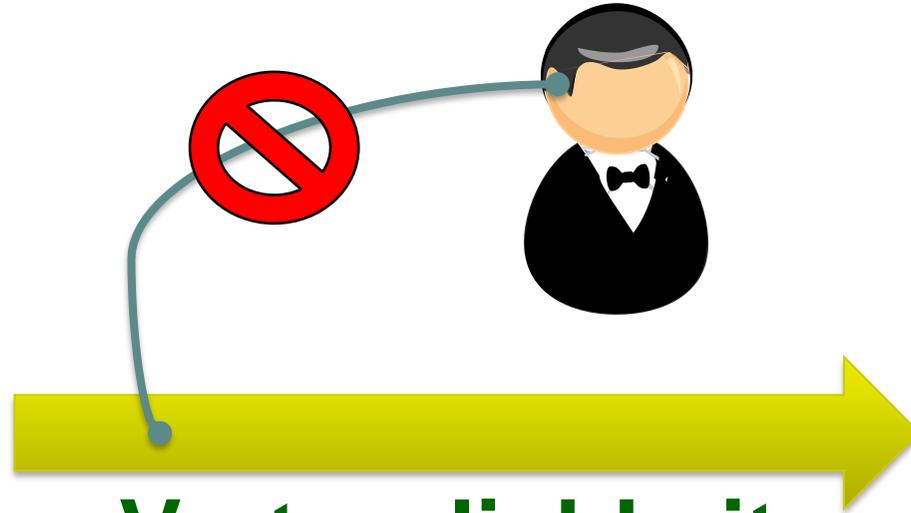
Dieses Werk steht unter der freien Lizenz [cc-by-sa-4.0](#) Information



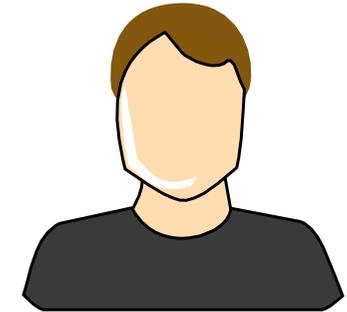
Sicherheitsziele



Alice



Vertraulichkeit
kein Mitlesen durch Fremde

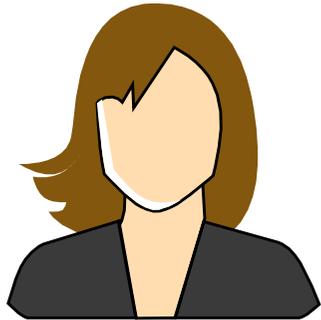


Bob

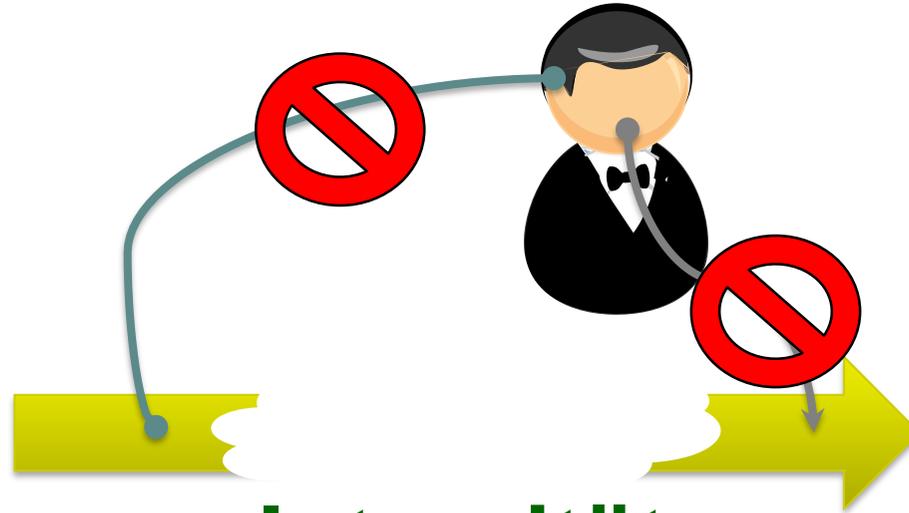
Verschlüsselung



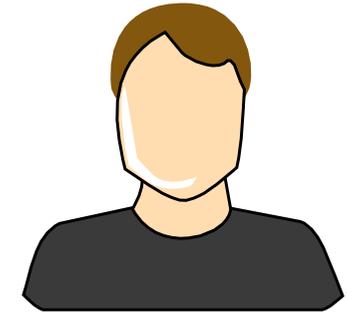
Sicherheitsziele



Alice



Integrität
keine Manipulation durch Fremde

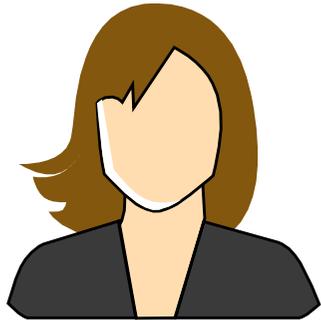


Bob

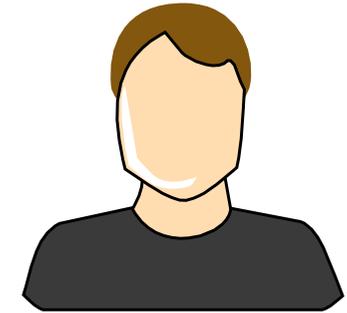
Versiegelter Brief



Sicherheitsziele



Alice



Bob

Authentizität

Nachricht ist definitiv vom
Absender.

Digitale Unterschrift



Sicherheitsziele





Grundbegriffe



Kryptologie/Kryptografie/Kryptoanalyse



Grundbegriffe



Klartext-/Geheimtext

Klartext-/Geheimtextalphabet



Grundbegriffe



Schlüssel



Klassische Verschlüsselung



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

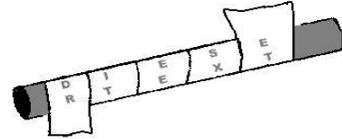


Nachrichten in unsichtbarer Tinte werden sichtbar, wenn sie von hinten erhitzt werden. Die Sicherheit hängt von absoluter Diskretion ab. Einfach zu entschlüsseln.

Kryptographie
(verschlüsseln)

Substitution

Transposition



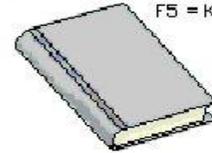
Chiffrierung

(Buchstaben ersetzen)

Codierung

(Wörter ersetzen)

Codes



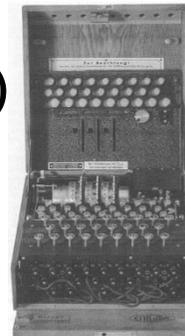
F5 = Komm heute Nacht zum Ahornbaum

Ohne Schlüsselcode lassen sich keine Nachrichten abfassen. Zum Entschlüsseln ist ein Codebuch notwendig.

Monoalphabetisch
(Captain Kidd, Caesar)



Polyalphabetisch
(Vigenère, Enigma)



one time pad

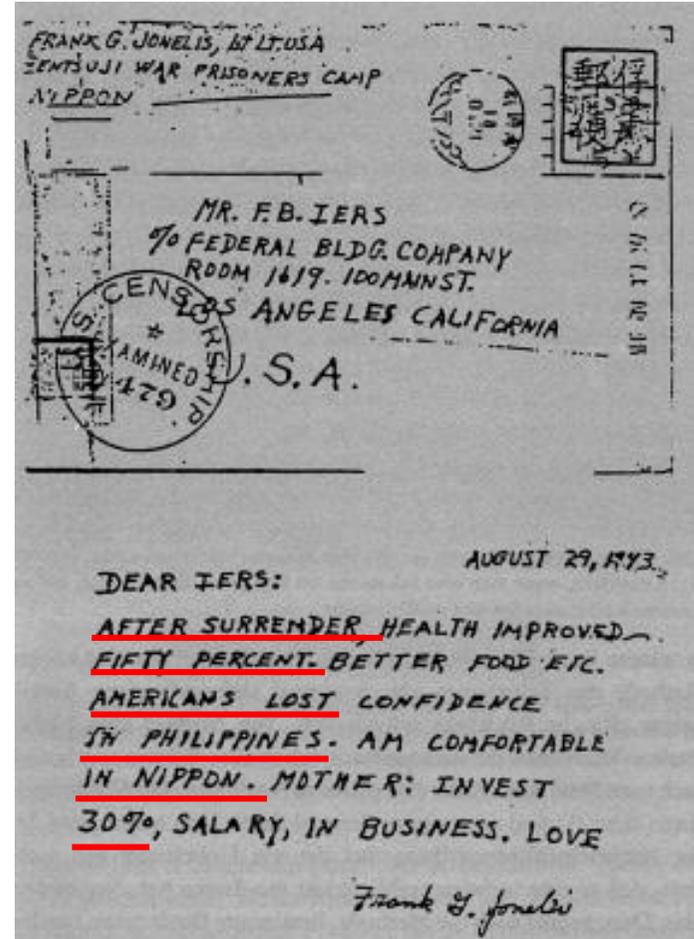




Steganografie



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

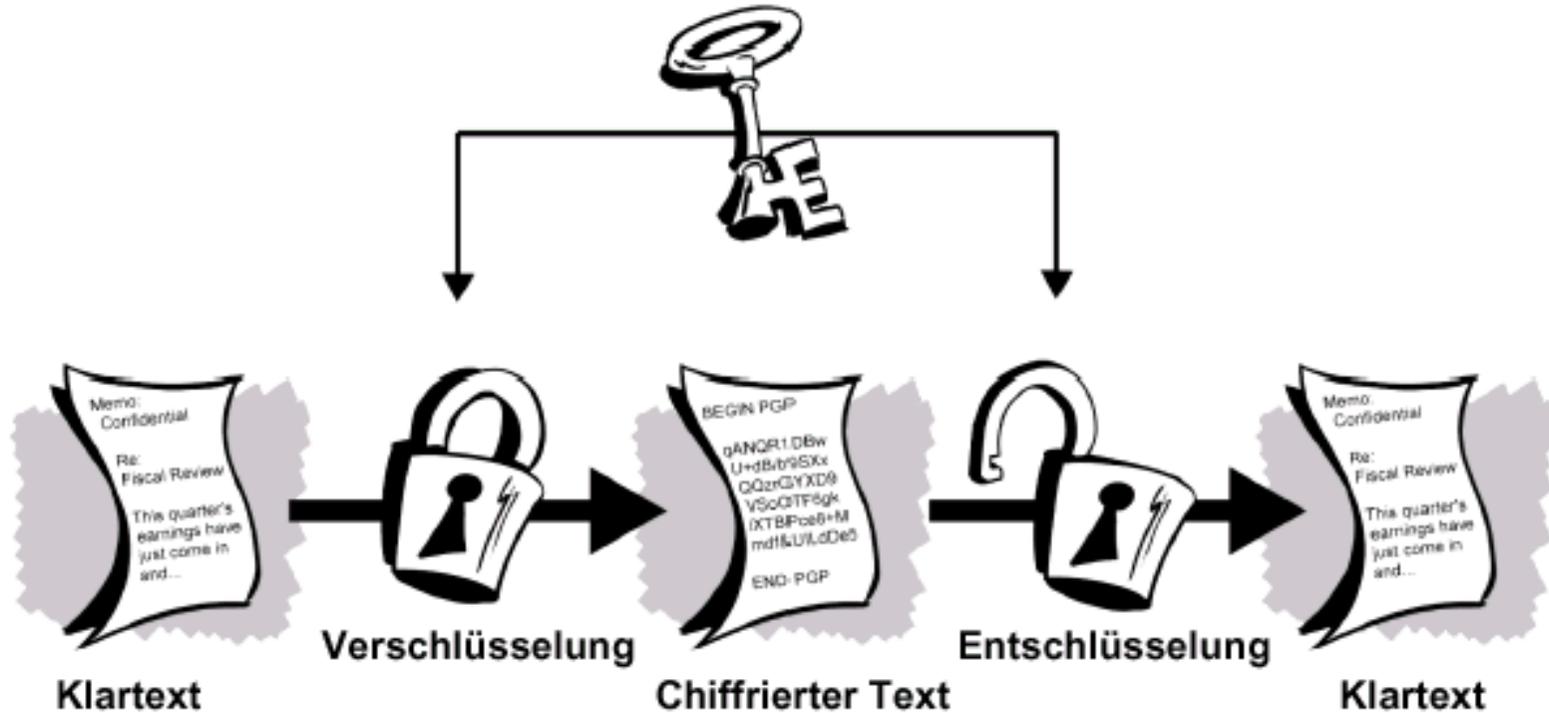


Quelle:

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.

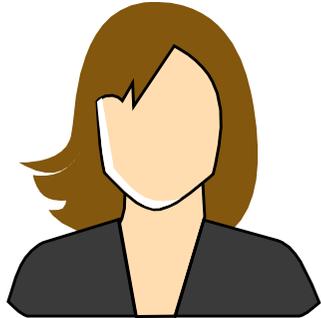
Station 3: POLYBIOS und PLAYFAIR

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

Station 5: Enigma (nur für Freaks!)



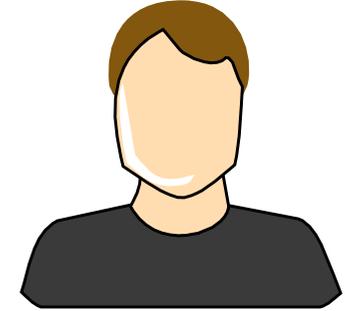
Grundproblem aller Verfahren



Alice



Mr. X



Bob

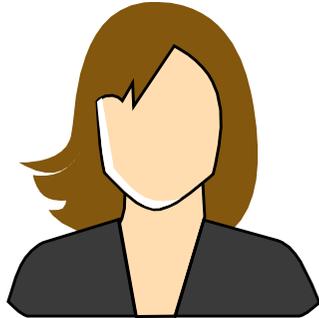
Hallo Bob!
Dein Schlüssel lautet
Hns1m2Glck.

Deine Alice!

Monoalphabetisch → statistische Angriffe



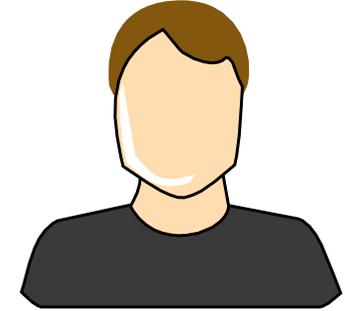
Grundproblem aller Verfahren



Alice



Mr. X



Bob

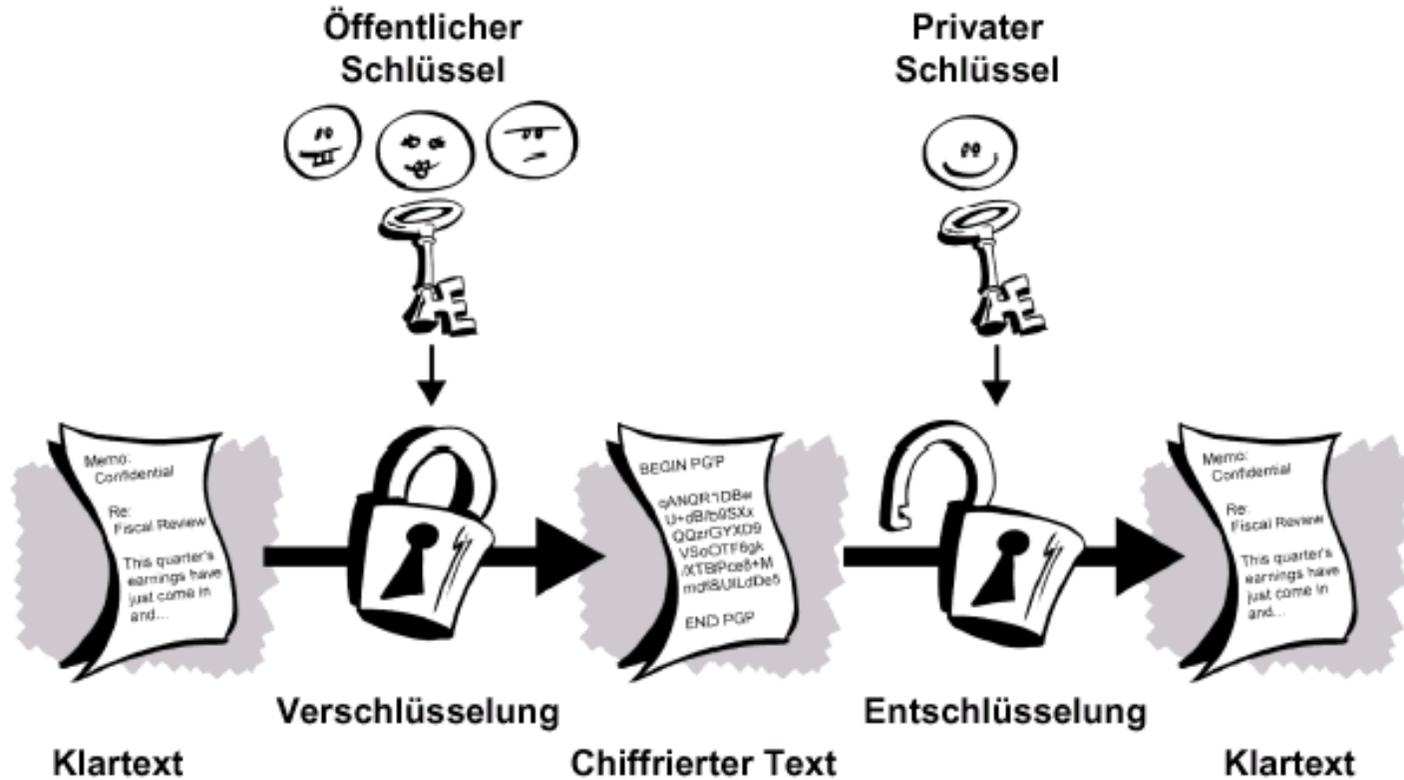
Hallo Bob!
Dein Schlüssel lautet
Hns1m2Glck.

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



Ein Pfund Gehacktes

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



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`.

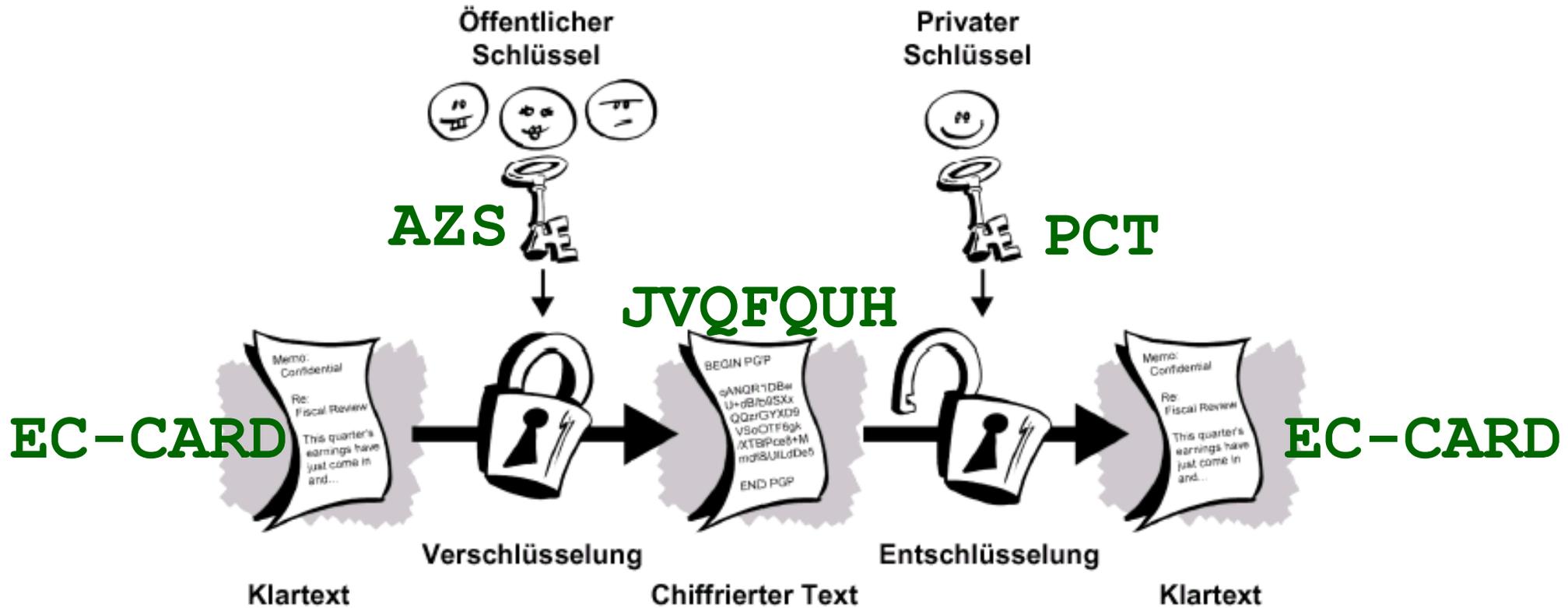
... und was passiert beim Schlüssel `PCT`?

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



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)

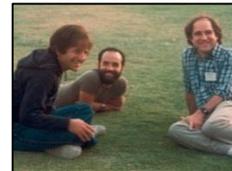
asymmetrisch
(Public Key, Diffie u. Hellmann)

Blockchiffrier-
algorithmen
DES

Stromchiffrier-
algorithmen
AES - WPA2



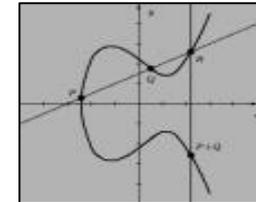
RSA
(Rivest, Shamir, Adleman)



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



Bob-AG entschlüsselt: **ACHTEINS**

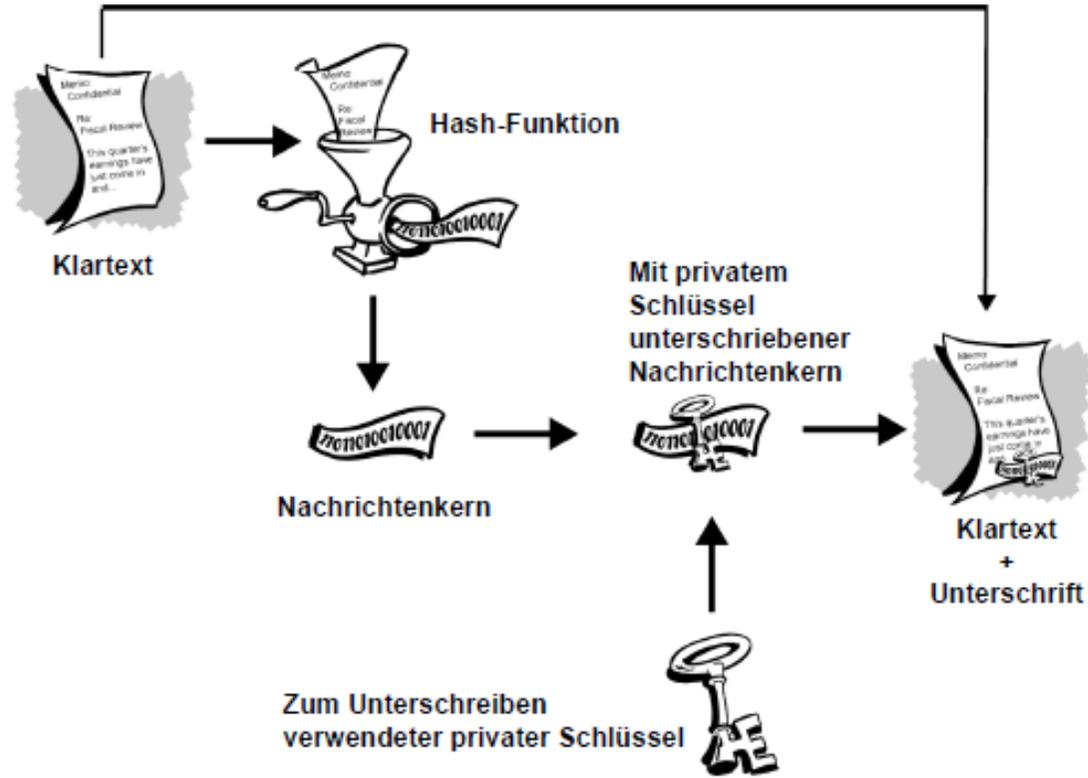
3 Alice erhält **OK H.** und entschlüsselt das zweite Wort zu **OK** mit dem Ergebnis **OK = OK**



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



Digitale Signatur



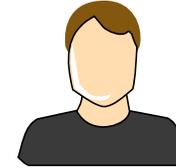
aus: Network Associates Inc. (Hrsg.): Handbuch "Einführung in die Kryptographie", Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.



Asymmetrische Verfahren



Alice **BGF**



Bob-AG

+: BGF
-: FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit

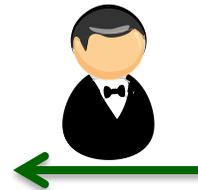
BGF

2 Alice verschlüsselt die 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 Bestätigung **OK** mit private key zu **H.**

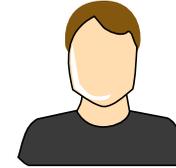
und sendet **OK** sowie das verschlüsselte **OK**



Asymmetrische Verfahren



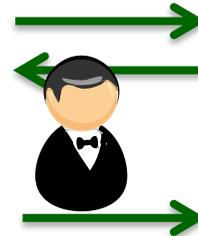
Alice **BGF**



Bob-AG

+: BGF
-: FDB

- 1 Alice fragt Bob-AG nach deren public key
- 2 Alice verschlüsselt die Kartennummer **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 Bestätigung **OK** mit private key zu **H.**

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



Asymmetrische Verfahren



Alice **BGF**



Bob-AG

+: BGF
-: FDB

BGF

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit

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 Bestätigung **OK** mit private key zu **H.** und sendet **OK** sowie das verschlüsselte **OK**



Asymmetrische Verfahren



Alice **CEF**



+: CEF
-: ZLB

BGF



Bob-AG

+: BGF
-: FDB

1 Alice fragt Bob-AG nach deren public key



Bob-AG antwortet mit

Bob-AG BGF

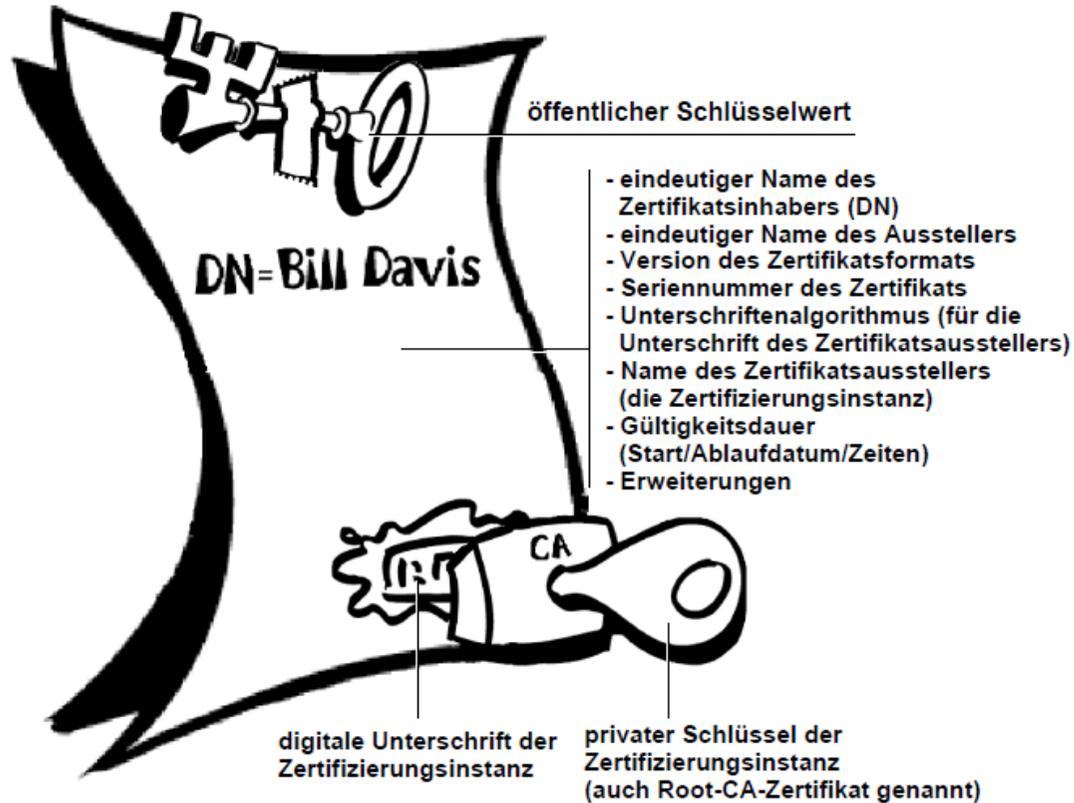
2 Alice verschlüsselt die Kartenummer **ACHTEINS** zu **LTLHN.WA** und sendet an Bob-AG



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

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



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

[Ausstellereklärung](#)

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](#)

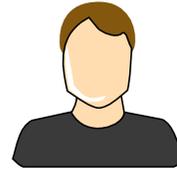
OK



Ausblick



Alice



Bob-AG

+: BGF
-: FDB



Alice

+: IKU
-: JUK



Bob-AG

+: BGF
-: FDB



E-Mail-Verschlüsselung



Schlüsseigenschaften

Primäre Benutzerkennung | Tino Hempel <T.Hempel@wossidlogymnasium.de>
Typ Schlüssel paar
Fingerabdruck 93CB 91CB 1278 E666 328F 6DDD 3DA4 1BBD ED86 D8B8

Allgemein **Zertifizierungen** Struktur

Benutzerkennung / Zertifiziert von	Fingerabdruck	Erzeugt am
▾ Tino Hempel <T.Hempel@wossidlogymnasium.de>	93CB 91CB 1278 E666 328F 6DDD 3DA4 1BBD ED86 D8B8	01.07.14
Tino Hempel <T.Hempel@wossidlogymnasium.de>	93CB 91CB 1278 E666 328F 6DDD 3DA4 1BBD ED86 D8B8	01.07.14
ct magazine CERTIFICATE <pgpCA@ct.heise.de>	A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000	10.09.15
Tino Hempel <T.Hempel@wossidlogymnasium.de>	93CB 91CB 1278 E666 328F 6DDD 3DA4 1BBD ED86 D8B8	01.07.14

Aktion wählen... ▾

Schließen



E-Mail-Verschlüsselung



Verfassen: Neuste Informationen daher geheim

Datei Bearbeiten Ansicht Optionen Enigmail Extras Hilfe

Senden | Rechtschr. | Anhang | S/MIME | Speichern

Enigmail: Meinen öffentlichen Schlüssel anhängen Nachricht wird unterschrieben und

Von: Tino Hempel <feedback@tinohempel.de> 1 Feedback

An: Lutz Hellmig <lutz.hellmig@uni-rostock.de>

An:

Betreff: Neuste Informationen daher geheim

1 Anhang
0xEA776AF3.asc

Enigmail-Bestätigung

Nachricht PGP/MIME UNTERSCHRIEBEN VERSCHLÜSSELT an folgende Empfänger senden:
lutz.hellmig@uni-rostock.de

Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:
0x38FD806FD5F51D2E



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/>