Die Welt der Verschlüsselung

Geheime Postkarten im Internet

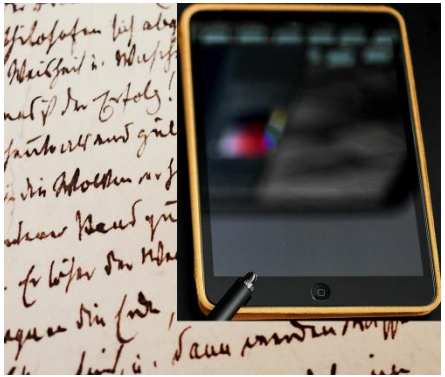
Prof. Bernhard Esslinger
bernhard.esslinger@uni-siegen.de
Sa 26. August 2017

Postaufkommen in Deutschland

- Briefe und Postkarten
  - knapp 16 Mrd. in 2015; fallende Tendenz
- Mails (mit und ohne Anhänge)(spam-bereinigt)
  - [redacted] in 2016; steigende Tendenz
- SMS
  - knapp [redacted] in 2016; stark fallende Tendenz
- Internet-Nachrichten / Instant Messaging / Chat-Dienste (WhatsApp, Skype, ICQ, Wire, Signal, Threema) (mit und ohne Anhänge)
  - steigende Tendenz; Nutzeranteil *noch* kleiner als bei Email; Relevanz/Sensibilität der Nachrichten geringer als bei Email; Schätzung: Anzahl allein bei WhatsApp in 2015: [redacted]

Wie kommt sie an – die Post?

Briefkasten → Auto / Bahn / Flugzeug / Schiff → Briefträger →



- am PC oder Smartphone
- im Browser oder im Email-Client

→ Provider → Internet → Provider →

web.de
gmx.de
aikq.de
posteo.de

gmail.com
hotmail.de
yahoo.de
yandex.ru

http://www.emailtester.de/freemail/anbieter.php

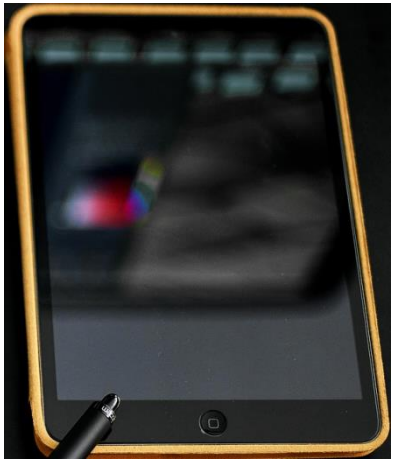
Verschlüsselte Postkarte

- Papierbasiert: zum Lesen muss man es physisch haben
  - Postkarten: Jeder Durchreicher (wieviele?) kann den Inhalt lesen
  - Brief: Zum Lesen muss man ihn öffnen
  - für beide: falls verschlüsselt genau abschreiben – schwarze Kammern angeblich schon ab 1464, sicher ab 1700 regelmäßig
- Internet-basiert: Anfertigen einer Kopie unterwegs fällt nicht auf
  - Normale E-Mail – wie eine Postkarte (oder ein geöffneter Brief)
  - Verschlüsselte E-Mail – Inhalt versteht nur der Empfänger
  - für beide: Falls verschlüsselt, einfach Kopie erstellen und – wie oben – anschließend versuchen zu knacken. „Schwarze Kammern“ wurden abgeschafft, Geheimdienste führten Überwachung ein.

Wo kann Email abgehört werden?

Gegen Massenüberwachung hilft nur Ende-zu-Ende-Verschlüsselung (E2E)

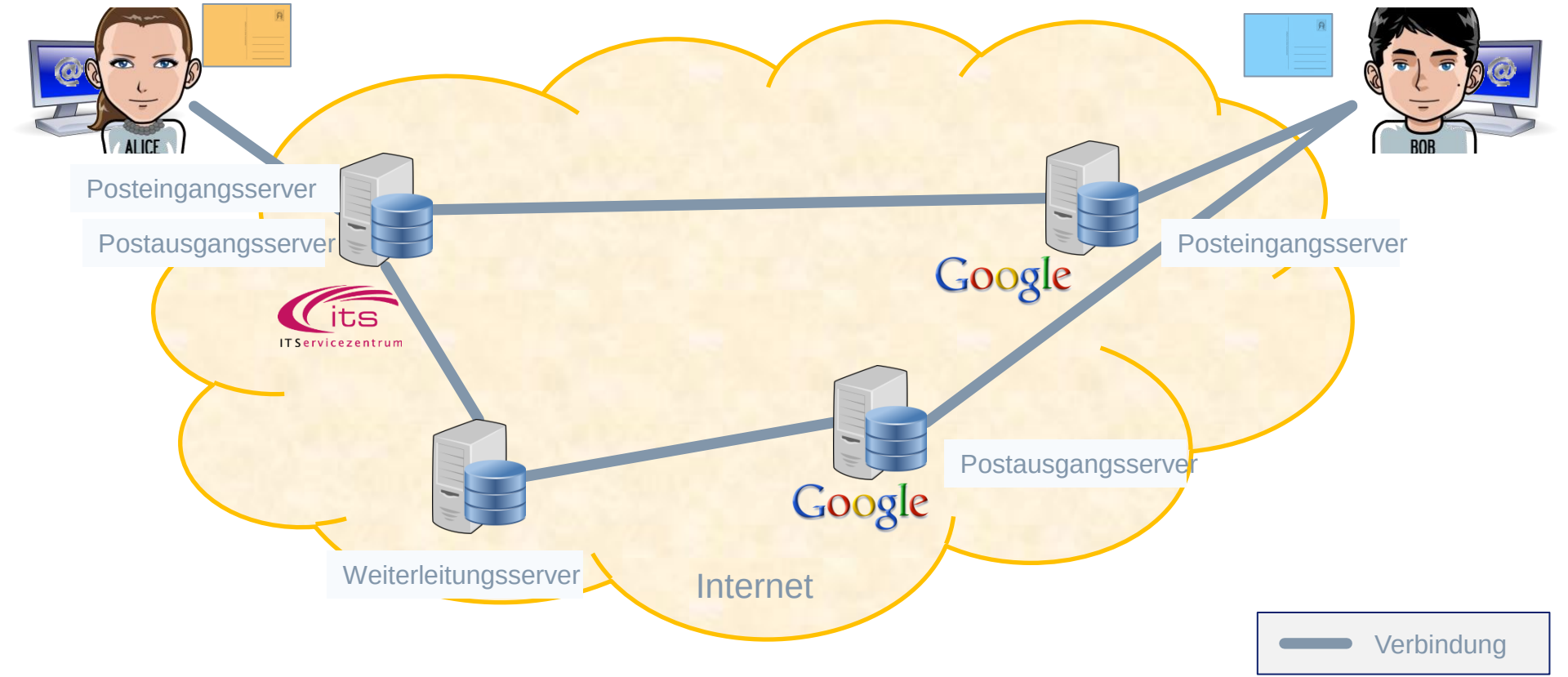
Provider → Internet → Provider



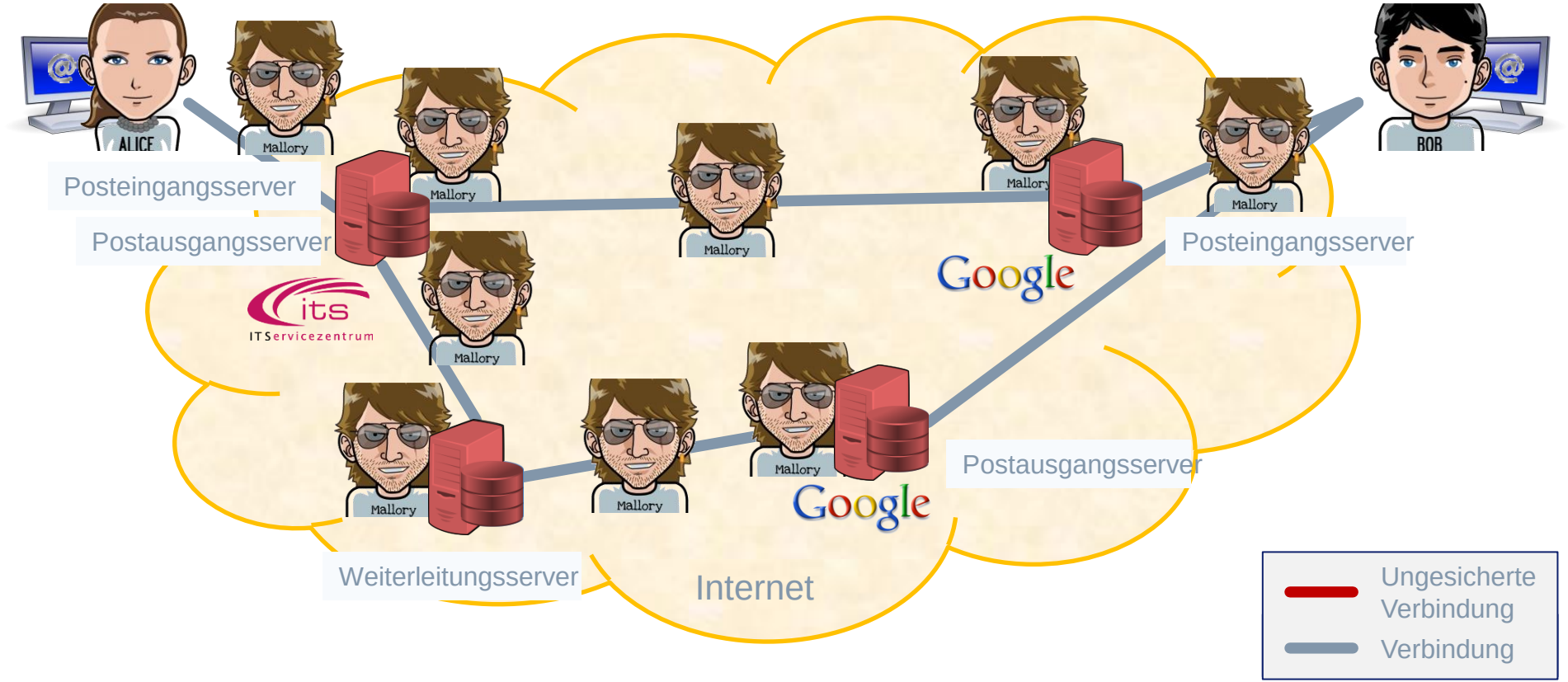
Massenüberwachung (Denic-Knoten, Unterseekabel, …)

Abhörmöglichkeit: überall

Wie funktioniert E-Mail?



Wer kann meine E-Mail lesen?



1. Lösung: Transportverschlüsselung: Verwendung von SSL/TLS

Zwischen Client und Server

- Provider muss es anbieten (IMAP**S**, POP3**S**, SMTP**S** , HTTP**S**)
- Benutzer kann/muss es selbst einschalten (Auswahl von SSL/TLS)

Zwischen den Servern

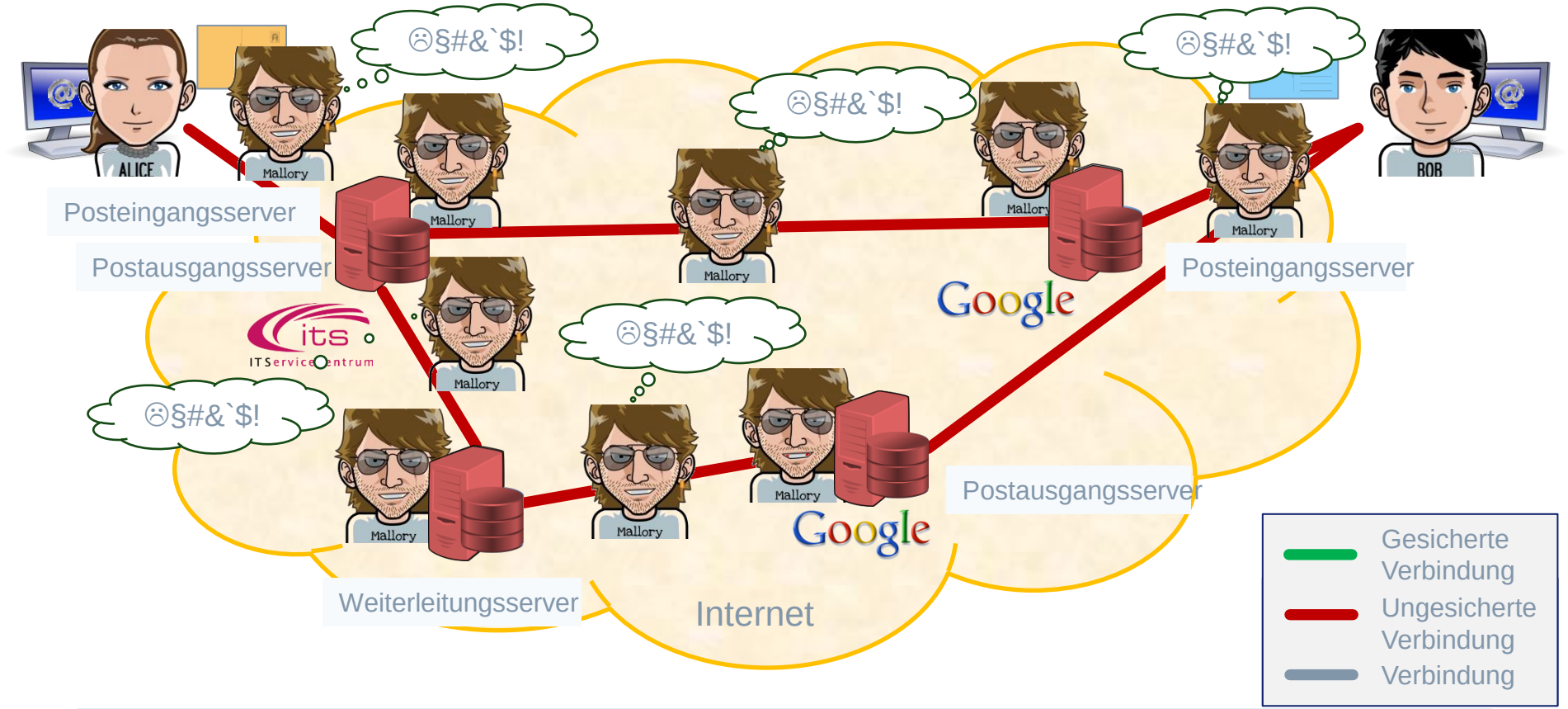
- Wird i.d.R. automatisch aktiviert, wenn von beiden Seiten unterstützt
- Bei Inkompatibilität wird stillschweigend die Sicherung abgeschaltet
- Benutzer hat keinen Einfluss darauf

Beispiele

- „E-Mail Made in Germany“
- De-Mail (ohne die diskutierte PGP-Verschlüsselung)
  (seit 2011; Linus Neumann: „Bullshit made in Germany“)

De-Mail

Auswirkung der Transportverschlüsselung



… und die wirkliche Lösung: Ende-zu-Ende-Sicherung

Bisher: Sicherung der Transportwege (Transportverschlüsselung)

- Auf jedem Server liegt der Klartext vor
- Manipulation der Daten, z.B. des Absendernamens, möglich (Spam)

Besser: Sicherung des Mailinhaltes (Ende-zu-Ende)

→ basiert auf asymmetrischer Kryptographie

Verschlüsselung der Daten und Signierung durch den Absender

— Daten sind auf dem gesamten Übertragungsweg nie unverschlüsselt

— Identität des Absenders und Integrität des Inhalts kann überprüft werden

Unabhängig von der Sicherung des Transportweges

Zwei Möglichkeiten (beides anerkannte Standards)

— S/MIME – Secure / Multipurpose Internet Mail Extensions (1995, RFC 2633)

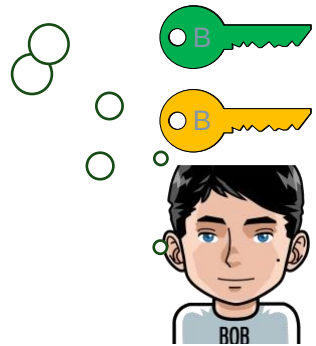
— OpenPGP – Pretty Good Privacy (1998, RFC 2440)

Grundlage: Asymmetrische Kryptographie – Verschlüsseln

Eine vertrauliche Nachricht an Bob verschlüssele ich mit **seinem öffentlichen** Schlüssel.

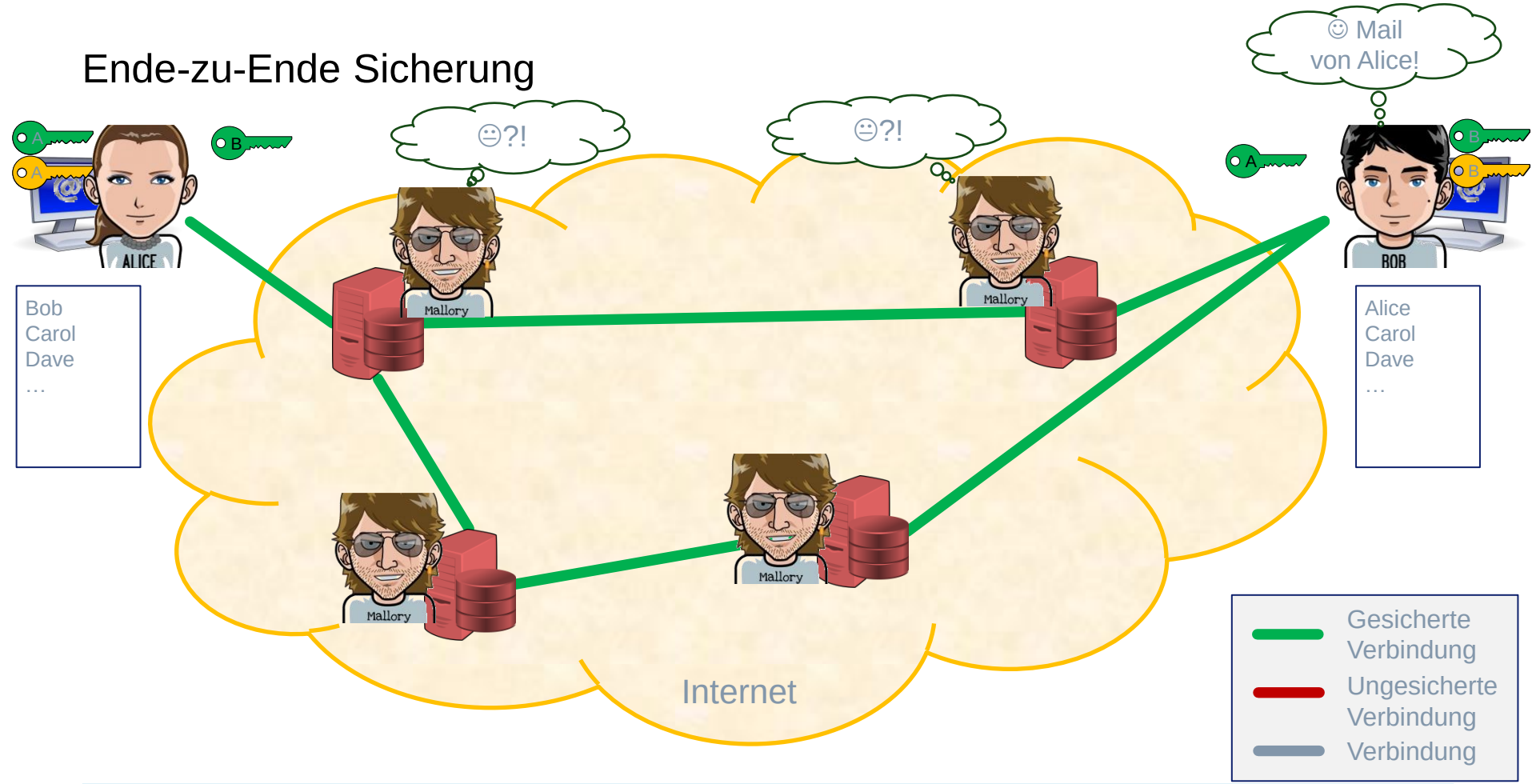
Eine vertrauliche Nachricht für mich entschlüssele ich mit **meinem privaten** Schlüssel.

Nachricht



Öffentlicher Schlüssel
Privater/geheimer Schlüssel

Ende-zu-Ende Sicherung



Zwischen-Fazit

Es gibt gute Gründe, sichere E-Mail zu verwenden.

Ein alltagstauglicher praktischer Einsatz ist machbar.

- **Signieren immer.**
- **Verschlüsseln, wenn möglich.**

Wirkungsvoll

- gegen Hacker und neugierige Administratoren
- gegen Massendatenspionage

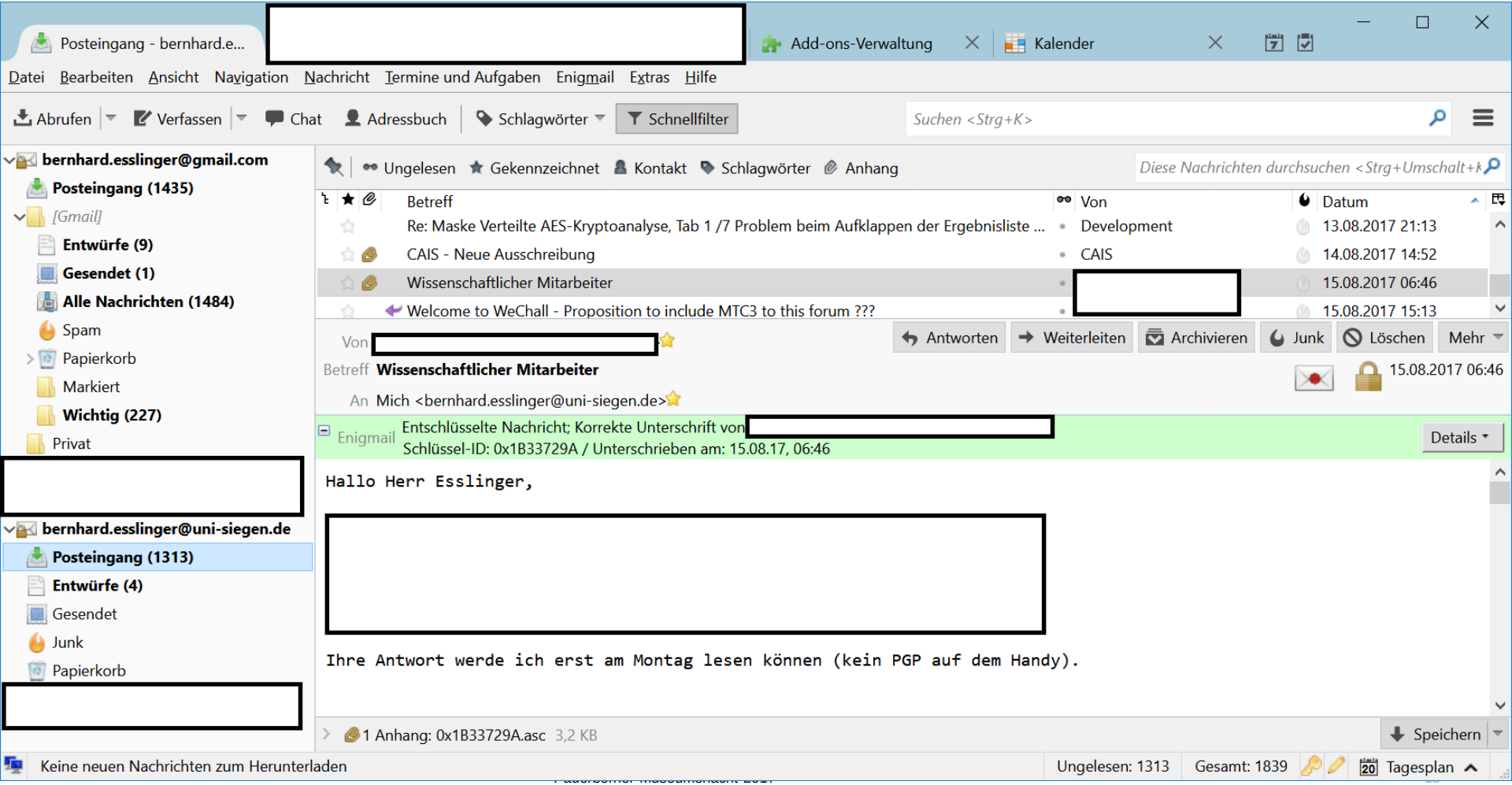
Wie nutzt man E2E-Verschlüsselung?

Browser (oder App)

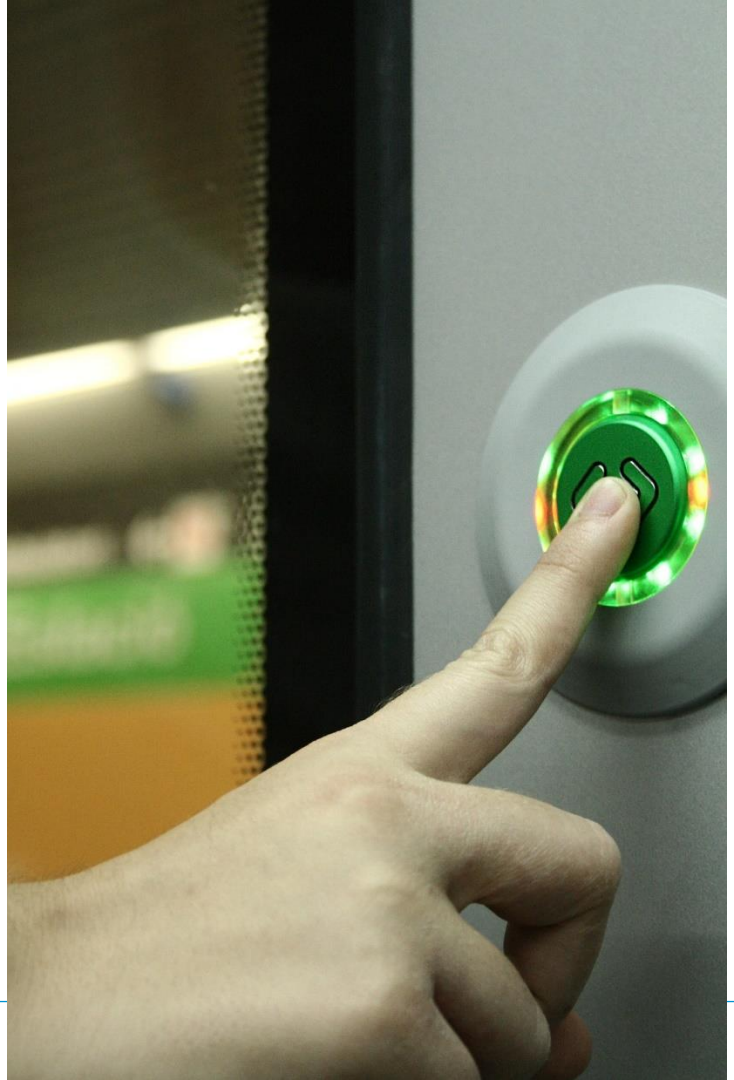
PGP per Plugin
(wie Mailvelope oder CryptUp)
(bspw. von web.de und gmx)

Email-Client

a) S/MIME ist schon eingebaut in die Email-Programme
b) PGP: per Plugin wie Enigmail (bspw. für Thunderbird)

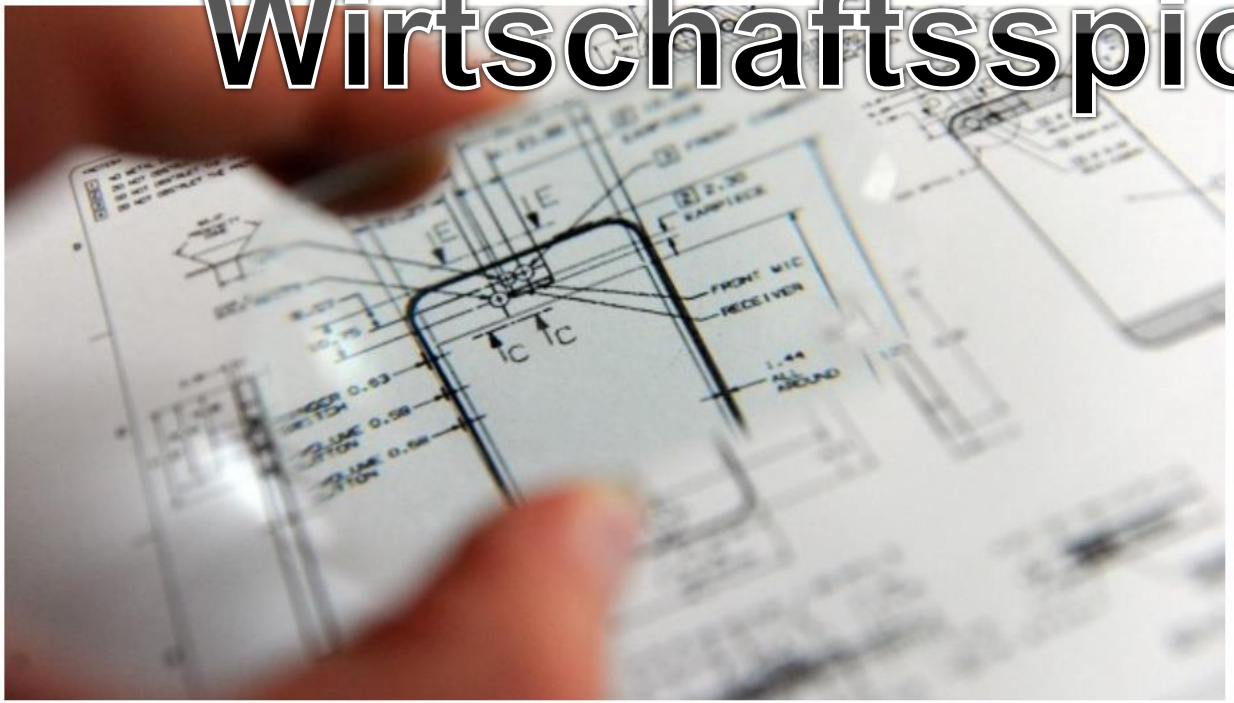

Posteingang - bernhard.e...
[redacted]
Add-ons-Verwaltung
Kalender
Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Enigmail Extras Hilfe
Abrufen Verfassen Chat Adressbuch Schlagwörter Schnellfilter
Suchen <Strg+K>
bernhard.esslinger@gmail.com
Posteingang (1435)
[Gmail]
Entwürfe (9)
Gesendet (1)
Alle Nachrichten (1484)
Spam
Papierkorb
Markiert
Wichtig (227)
Privat
[redacted]
bernhard.esslinger@uni-siegen.de
Posteingang (1313)
Entwürfe (4)
Gesendet
Junk
Papierkorb
[redacted]
Ungelesen Gekennzeichnet Kontakt Schlagwörter Anhang
Diese Nachrichten durchsuchen <Strg+Umschalt+K
Betreff Von Datum
Re: Maske Verteilte AES-Kryptoanalyse, Tab 1 /7 Problem beim Aufklappen der Ergebnisliste ... Development 13.08.2017 21:13
CAIS - Neue Ausschreibung CAIS 14.08.2017 14:52
Wissenschaftlicher Mitarbeiter [redacted] 15.08.2017 06:46
Welcome to WeChall - Proposition to include MTC3 to this forum ??? 15.08.2017 15:13
Von [redacted]
Antworten Weiterleiten Archivieren Junk Löschen Mehr
Betreff Wissenschaftlicher Mitarbeiter
15.08.2017 06:46
An Mich <bernhard.esslinger@uni-siegen.de>
Enigmail Entschlüsselte Nachricht; Korrekte Unterschrift von [redacted]
Schlüssel-ID: 0x1B33729A / Unterschrieben am: 15.08.17, 06:46
Details
Hallo Herr Esslinger,
[redacted]
Ihre Antwort werde ich erst am Montag lesen können (kein PGP auf dem Handy).
1 Anhang: 0x1B33729A.asc 3,2 KB
Speichern
Keine neuen Nachrichten zum Herunterladen
Ungelesen: 1313 Gesamt: 1839
Tagesplan

Awareness



Pixabay

Wirtschaftsspionage



© DPA

„Jahr für Jahr entstehen der deutschen Wirtschaft Schäden in Höhe von rund 50 Milliarden Euro, wobei die Dunkelziffer deutlich höher liegen dürfte“, sagte BDI-Präsident Ulrich Grillo.

Pflicht

- Backup
- Updates
- Menschenverstand

➔ … am Stand …

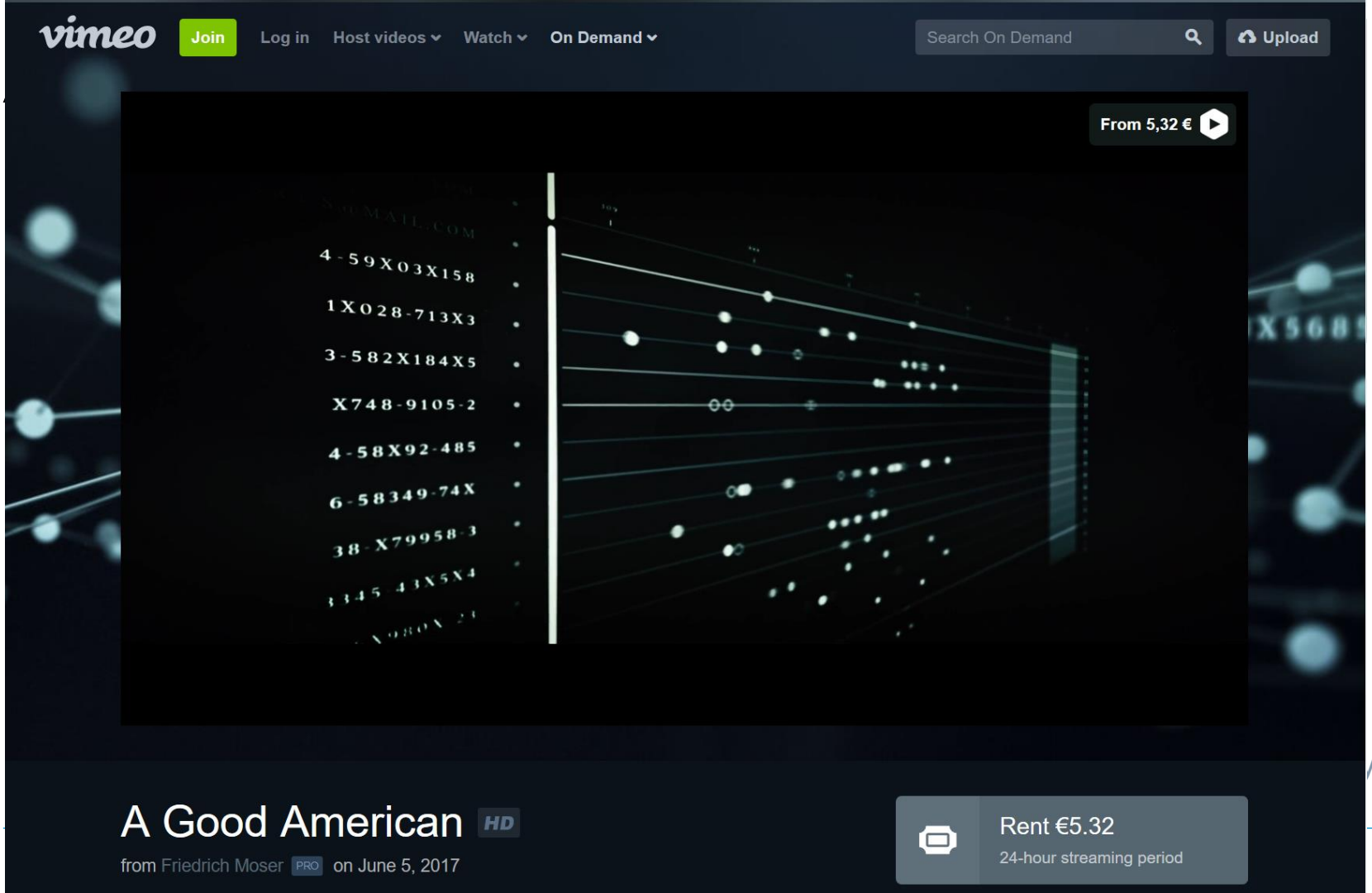
Pixabay

Kür → weitere Links + Details (im Anhang dieser Präsentation + am Stand im HNF)

- Machen Sie sich schlau
- Besuchen Sie eine CryptoParty
- Nutzen Sie E2E-Verschlüsselung
- Schauen Sie “A Good American”
- Spielen Sie mit den kostenlosen CrypTool-Programmen
- Lösen Sie Rätsel wie bei MTC3
- Treten Sie für Ihr Recht auf Privatsphäre ein

CrypTool

Pixabay


vimeo
Join
Log in
Host videos
Watch
On Demand
Search On Demand
Upload
From 5,32 €
4-59X03X158
1X028-713X3
3-582X184X5
X748-9105-2
4-58X92-485
6-58349-74X
38-X79958-3
A Good American
HD
from Friedrich Moser
PRO
on June 5, 2017
Rent €5.32
24-hour streaming period

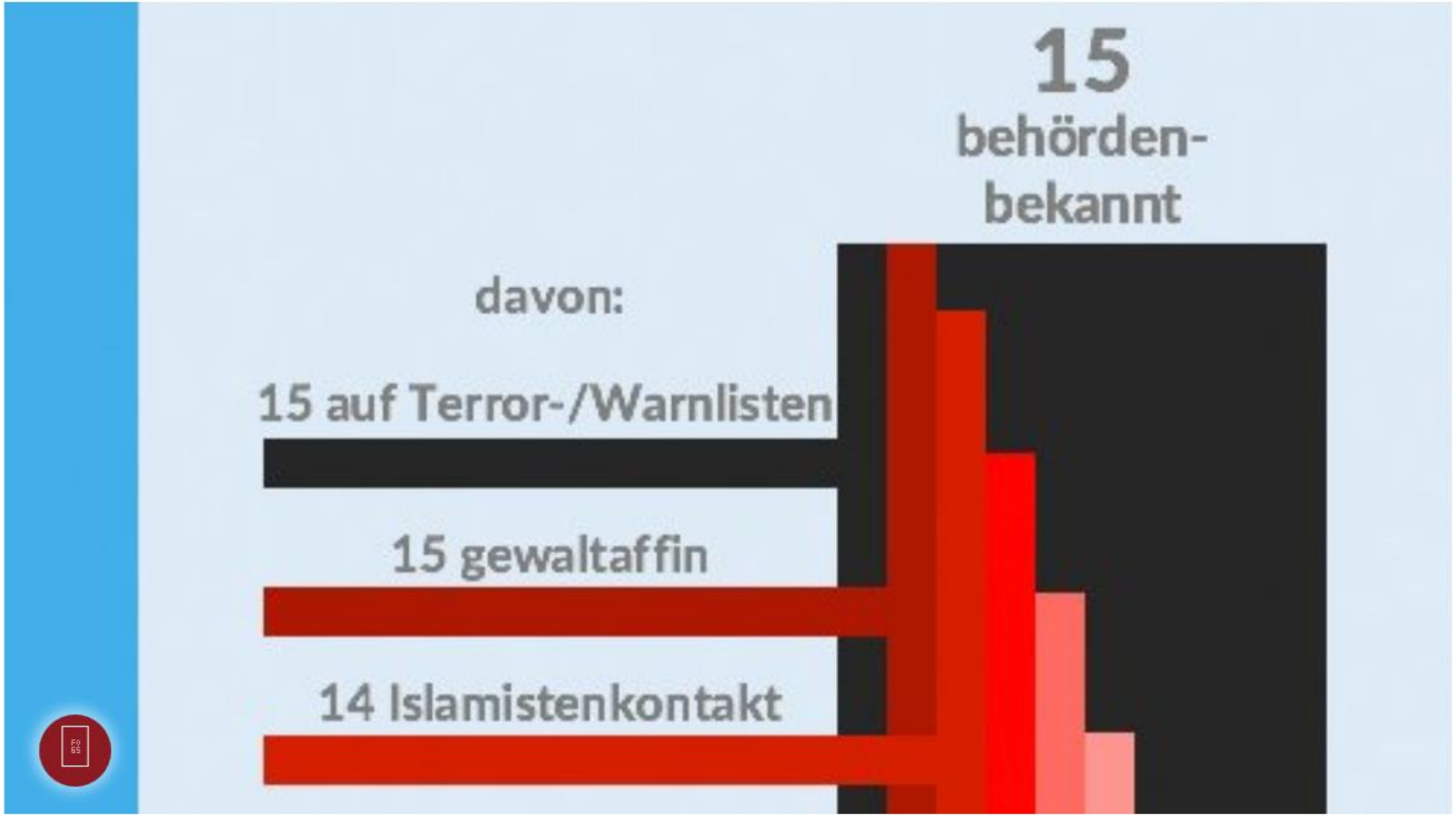
Terrorjagd im Netz

arte

SENDETERMINE

Dienstag, 12. September um 20.15 Uhr

Livestream: ja


15
behörden-
bekannt
davon:
15 auf Terror-/Warnlisten
15 gewaltaffin
14 Islamistenkontakt
saschalobo.com

Gute Verschlüsselung ist nicht knackbar.

Ich kann Tipps geben, wie ihr eure Kommunikation schützen könnt.

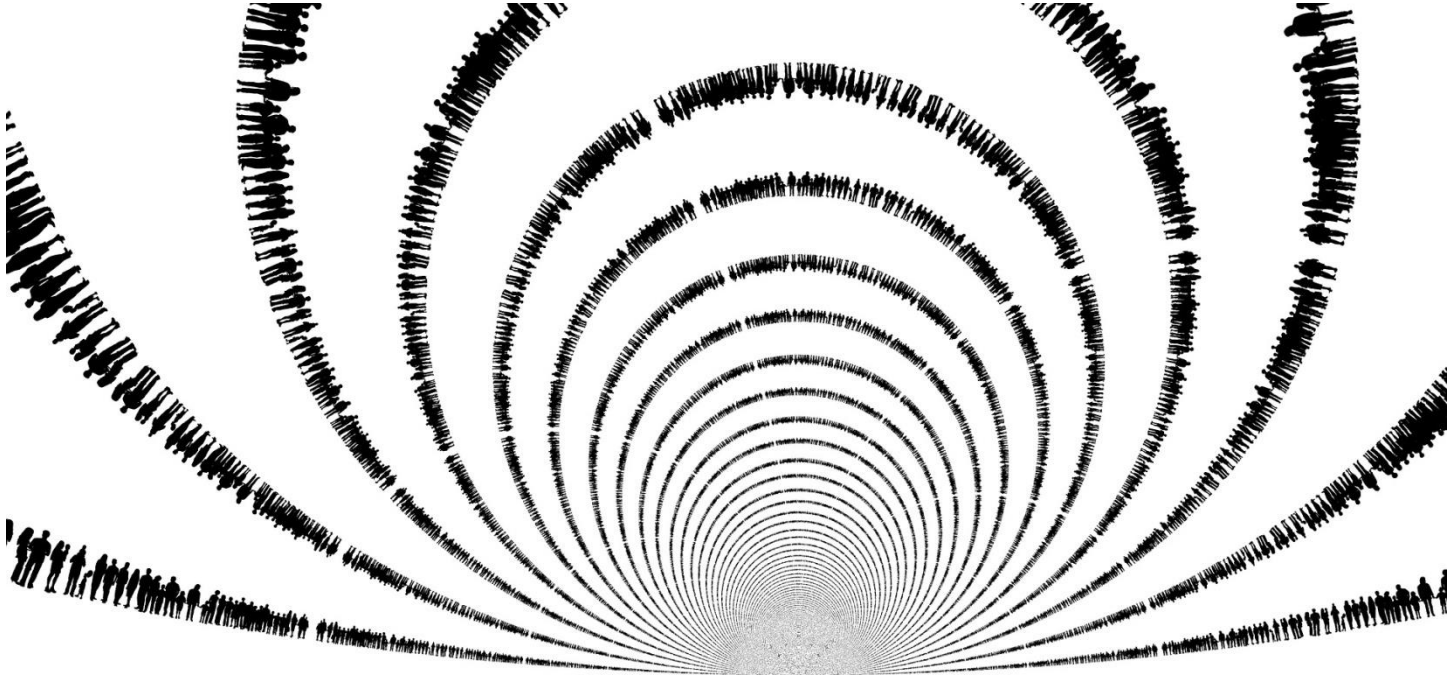
Aber das ist ein Kampf, den ihr so nicht gewinnen könnt.

Ihr müsst ihn auf den Titelseiten führen.

Zitat von Edward Snowden
Aus dem Interview mit Dan Gillmor — Süddeutsche Zeitung (2016)

Anhang für den Stand

- A
- B
- C



https://www.privacytools.io/

Pixabay

Technik verstehen – Verhalten ändern

Informationen zur Umsetzung – Beispiele

— **Sichere Email auf Smartphone oder PC (mit S/MIME oder OpenPGP)**

https://www.anti-prism-party.de/

https://www.anti-prism-party.de/downloads/sichere-email-am-pc-und-mit-dem-smartphone-anleitung.zip

— **Verschlüsselte Messenger**

https://www.anti-prism-party.de/downloads/instant-messaging-flyer.pdf

https://wire.com/de/ **Wire hat sehr gute Sprachqualität; für PC und Smartphone; kostenlos**

— **Wie surfe ich anonym? Wie kann man sicher mit sozialen Netzen umgehen?**

https://www.anti-prism-party.de/downloads/anonymes-surfen-flyer.pdf

https://www.anti-prism-party.de/downloads/soziale-netzwerke-flyer.pdf

Gesellschafts-politische Zusammenhänge – Verstehen und Einfluss nehmen

Informationen zur Vertiefung – Beispiele

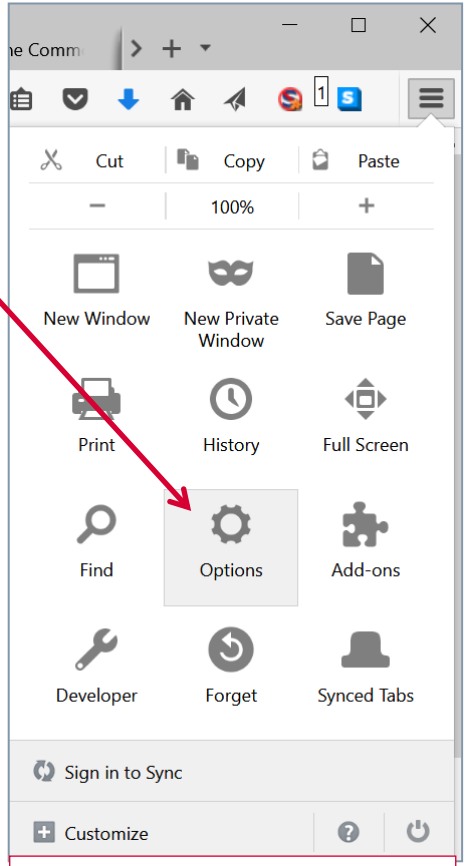
Ansehen

https://www.youtube.com/watch?v=iHlzsURb0WI	**Comics zu Überwachung, 11 min**
https://www.youtube.com/watch?v=d1qOkJcn2c4	**Vortrag Sascha Lobo zu Überwachung, 1h**
https://www.youtube.com/watch?v=tFrLKMu0UYk	**Interview mit Sascha Lobo, 1 h**
https://www.youtube.com/watch?v=QtvmjovN2Z0	**Arte Doku: Überwachung Total, 1,5 h**

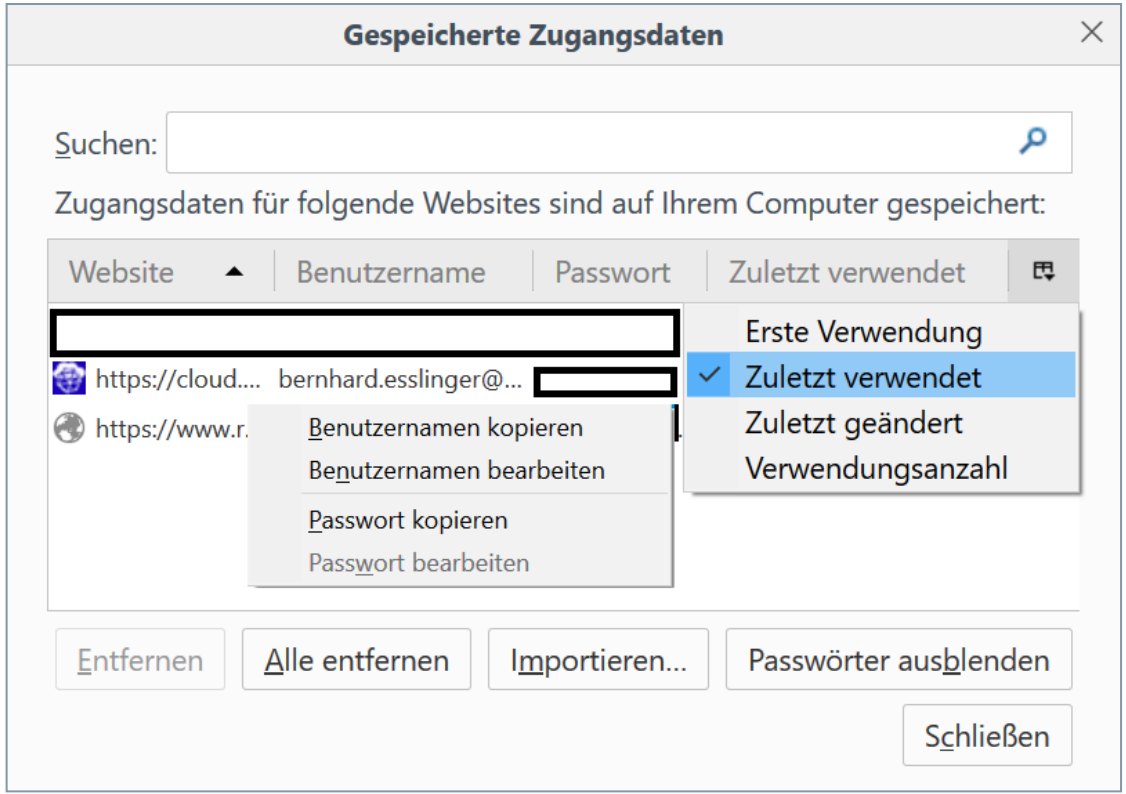
Aktiv werden,

- **damit Menschen wie Bill Binney und Edward Snowden gehört werden:**
  Um erfolgreich zu sein, müssen Geheimdienste gerade nicht ALLES sammeln.
- **damit ein fairer Ausgleich zwischen Sicherheit und Privatsphäre gefunden wird,**
  und klar machen, dass immer mehr Überwachung nicht mehr Sicherheit bedeutet.
- **damit auch Menschen wie Edward Snowden in Deutschland Asyl bekommen.**

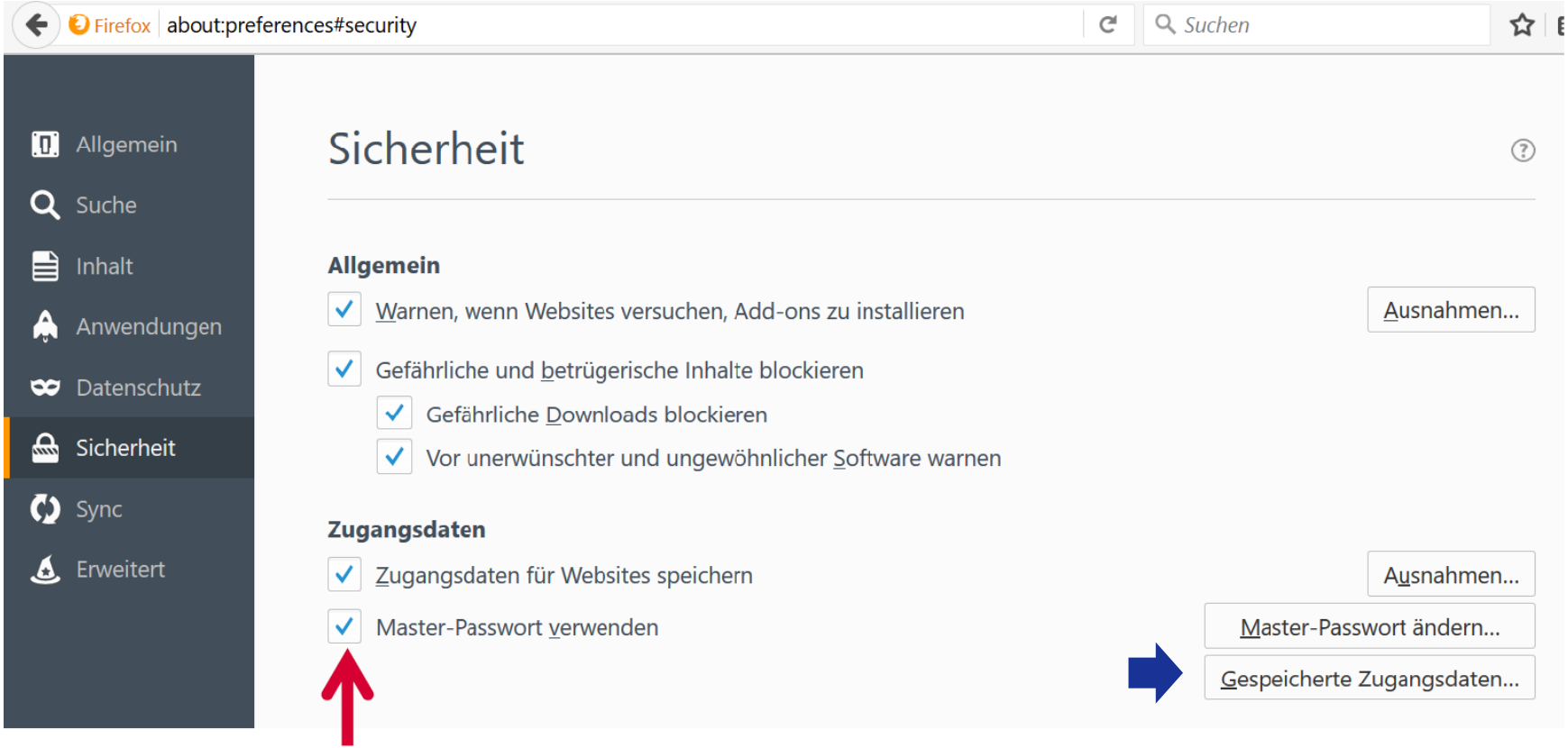
Nutzen Sie einen Passwortspeicher?



Firefox: Optionen, Sicherheit, Gespeicherte Logins



Jeder Passwort-Speicher braucht eine Zugangssicherung



Herausforderungen in der Praxis bei sicherer E-Mail

Technologien sind vorhanden, Benutzbarkeit ist deutlich zu verbessern.

Benutzbarkeit der existierenden Software ist unzureichend

Anfangshürde ist derzeit zu hoch (Zertifikat beantragen und Software einrichten)

Benutzer haben mehrere Geräte (Verteilung der Zertifikate auf alle Geräte)

Im Betrieb z.T. explizites Einschalten der Sicherung notwendig (1 Klick zu viel)

Ablauf/Erneuerung der Zertifikate (bei S/MIME) (eigene, alte Zertifikate behalten)

Interoperabilität …

… zwischen Mailclients

… zwischen den beiden etablierten Standards S/MIME und PGP

Staatliche Forschungsförderung sollte nicht bei Papers und Prototypen aufhören!

Lösungsansätze für sichere E-Mail

Es funktioniert bereits heute in großen Unternehmen

Sichere E-Mail wird den Mitarbeitern ohne Hürde angeboten und regelmäßig verlängert.

Gängige Lösungen verwenden zwei Schlüsselpaare (signieren und verschlüsseln)

- S/MIME Gateways (d.h. der Benutzer bemerkt davon nichts)
- Plugins für gängige E-Mail-Clients sind leider z.T. proprietäre Eigenentwicklungen

Sichere E-Mails soll in Zukunft auch für jedermann verfügbar sein

Automatisierte und kostenlose Zertifikate (direkt während der E-Mail-Einrichtung)

Automatisierte Verteilung der Zertifikate auf alle Geräte (z.B. durch einen Cloud-Dienst)

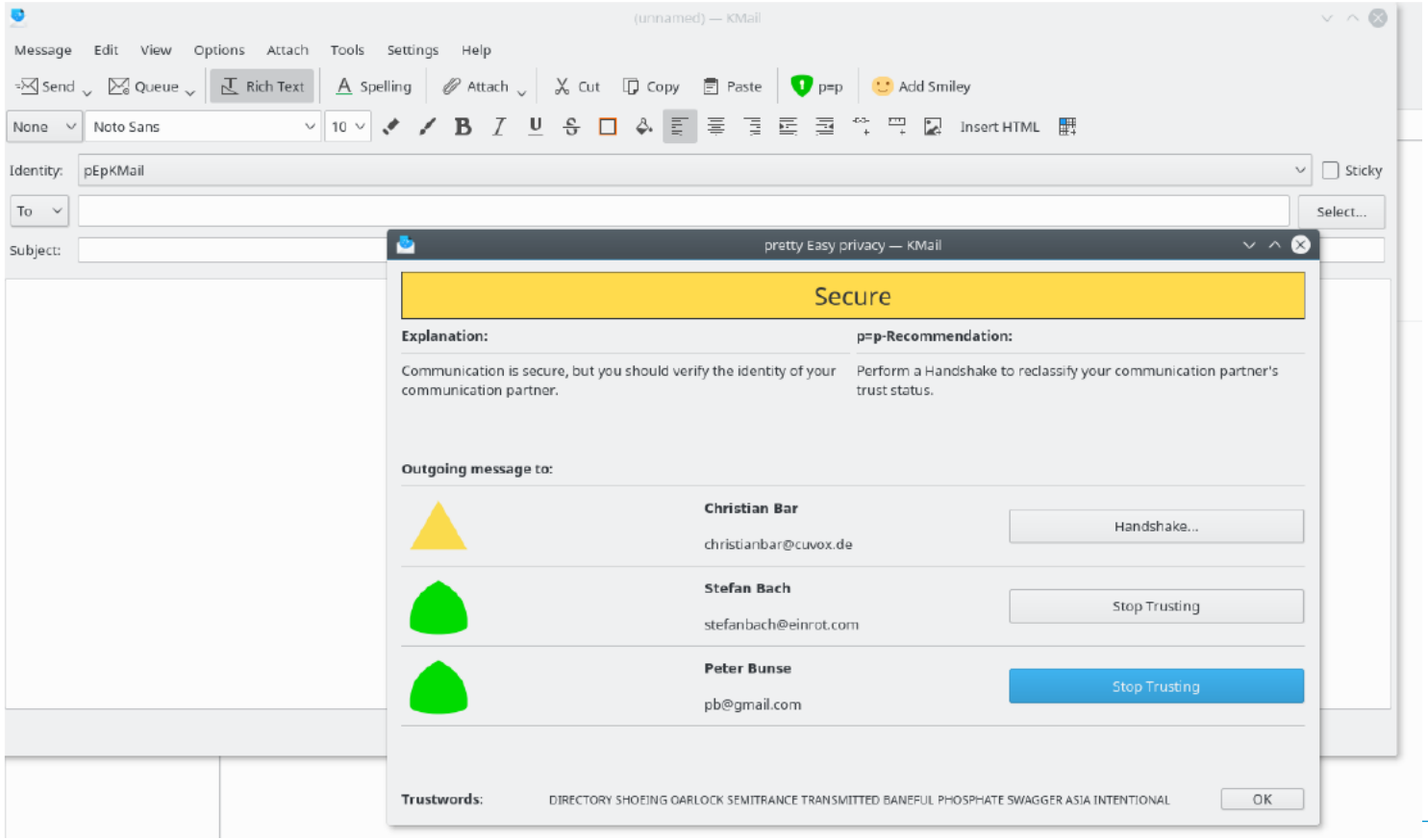
Nahtlose und konfliktfreie Integration der beiden Standards in alle E-Mail-Clients

Klare und einfache Rückmeldungen an den Benutzer

- ➔ **Für den Nutzer darf sich nichts ändern** (er will doch „nur“ eine E-Mail schreiben)
- ➔ Staat investiert in Standards statt in Lobby-getriebene, nationale „Sonderlocken“.

Ziel: Kein Expertenwissen nötig, nur Ampelsystem lesen + Absicht kundtun.

Abbildung 11: Fertiger Prototyp von pEp in KMail



Links zu den im Vortrag erwähnten Initiativen und Programmen

- MysteryTwister C3 (MTC3)

  www.mysterytwisterc3.org

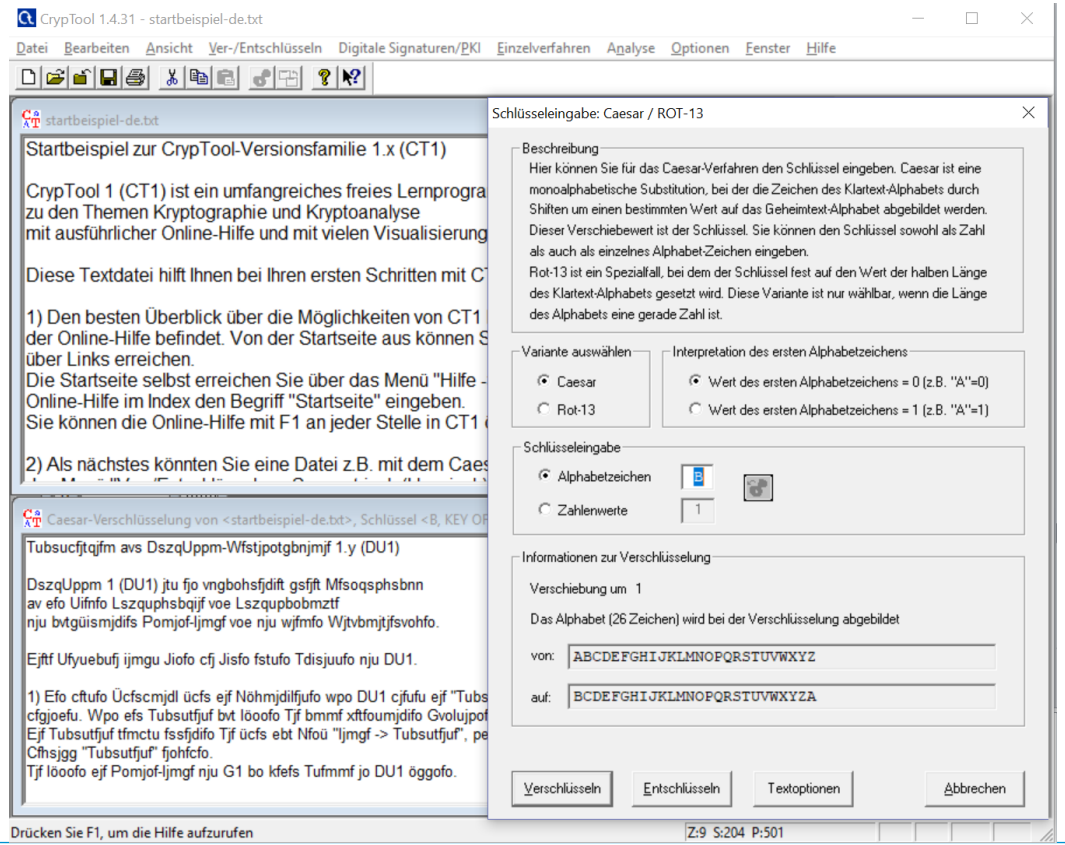
  Die Seite mit den Rätseln (u.a. die Postkarte von Lucy)

- CrypTool

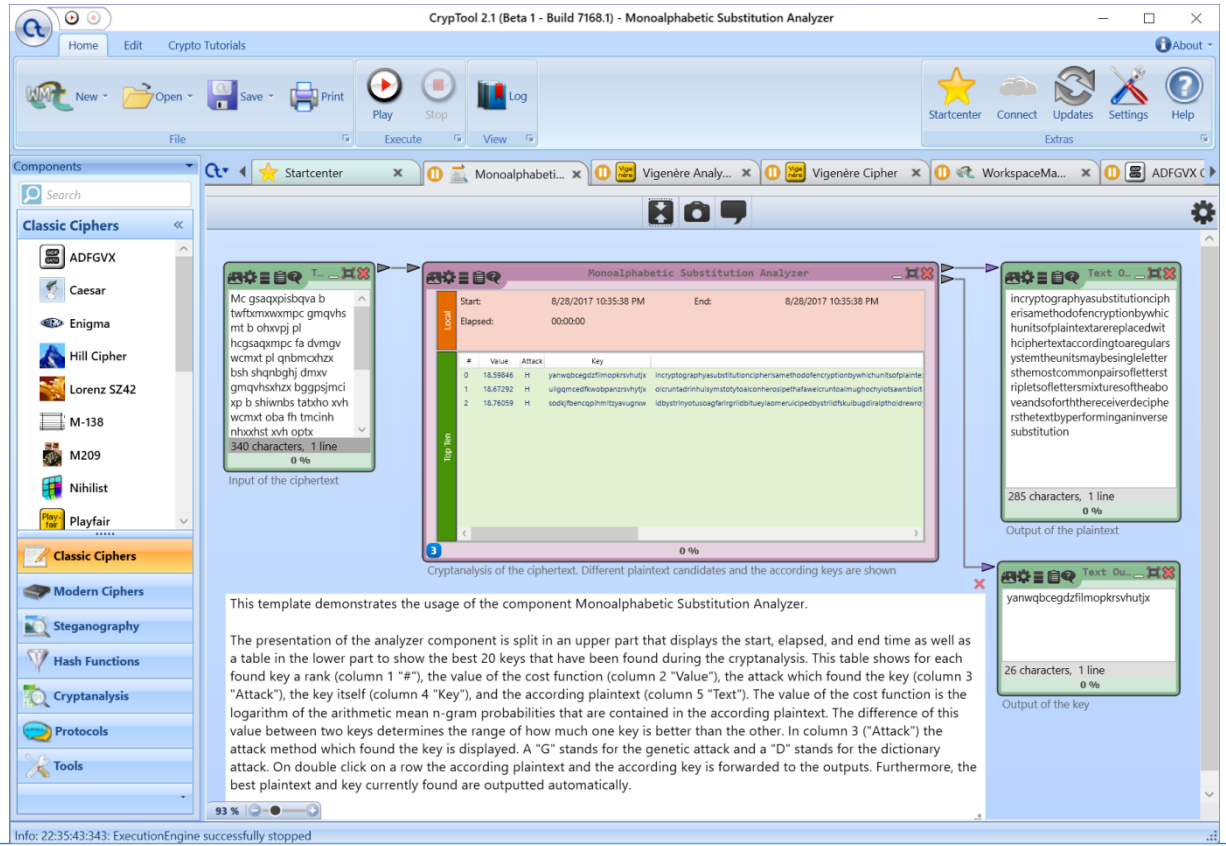
  www.cryptool.org

  Lernprogramme für Verschlüsselung und Kryptoanalyse

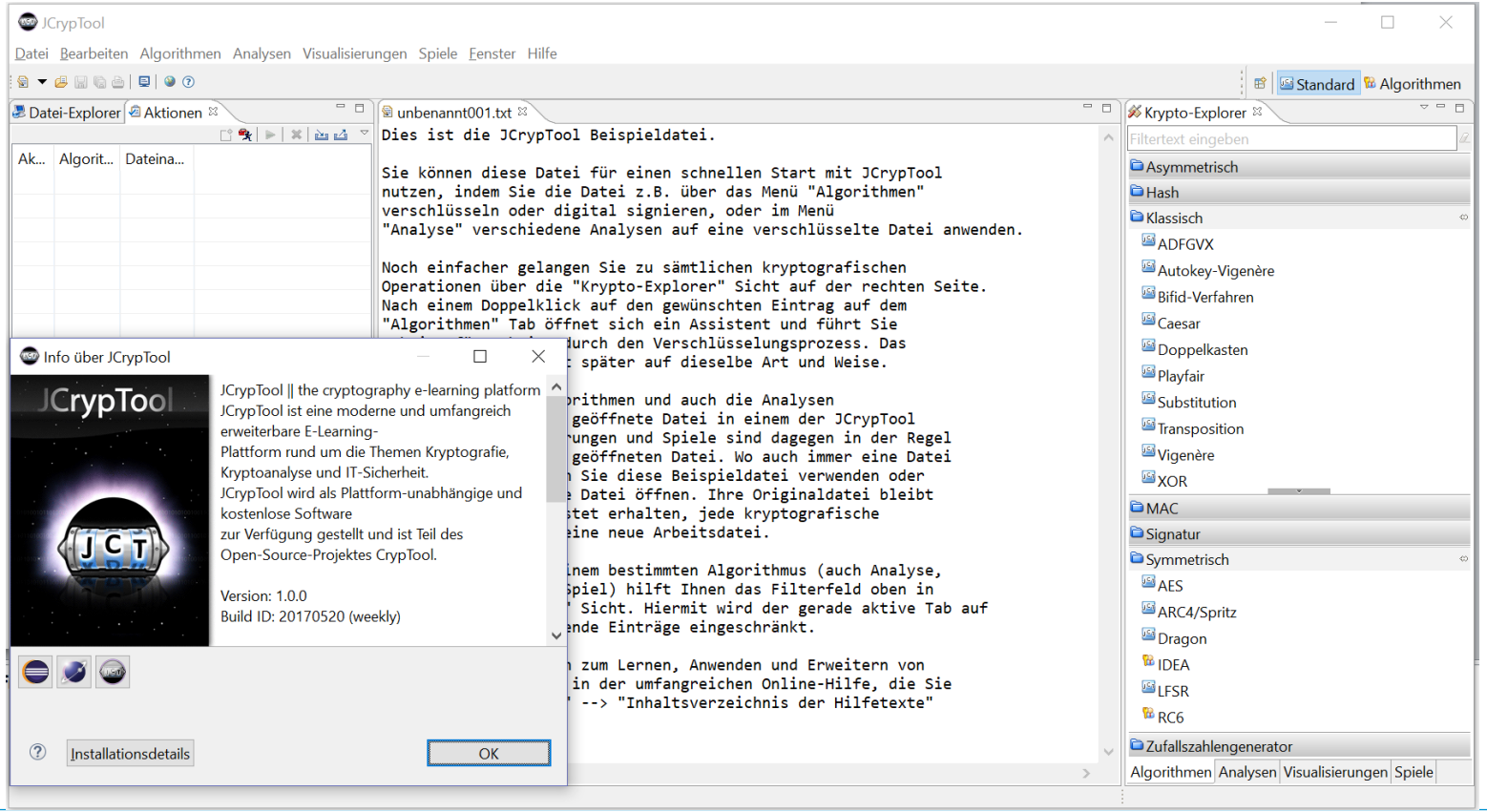
Screenshot zu CrypTool 1: Beispiel Caesar-Verschlüsselung



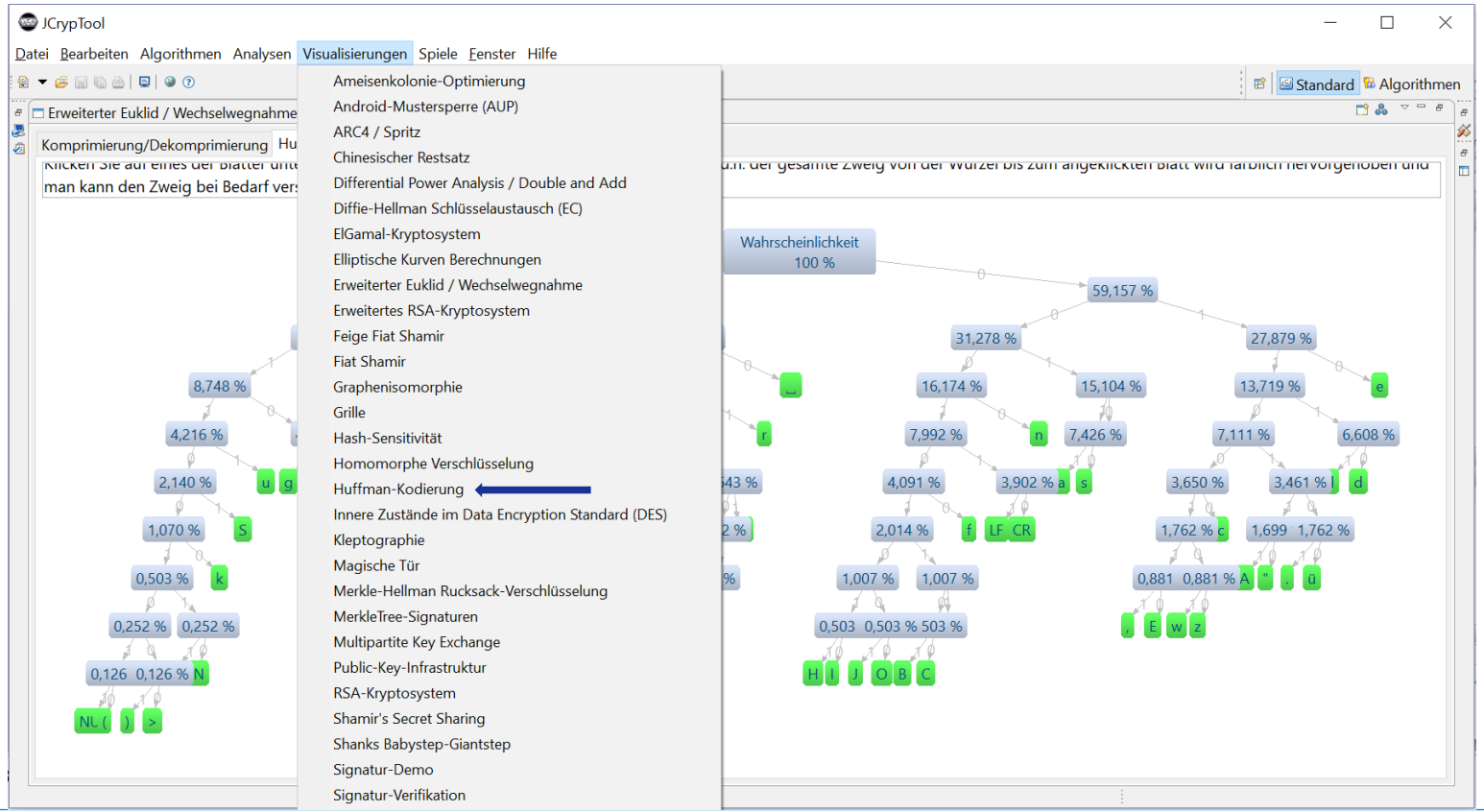
Screenshot zu CrypTool 2: Beispiel zur automatischen Analyse



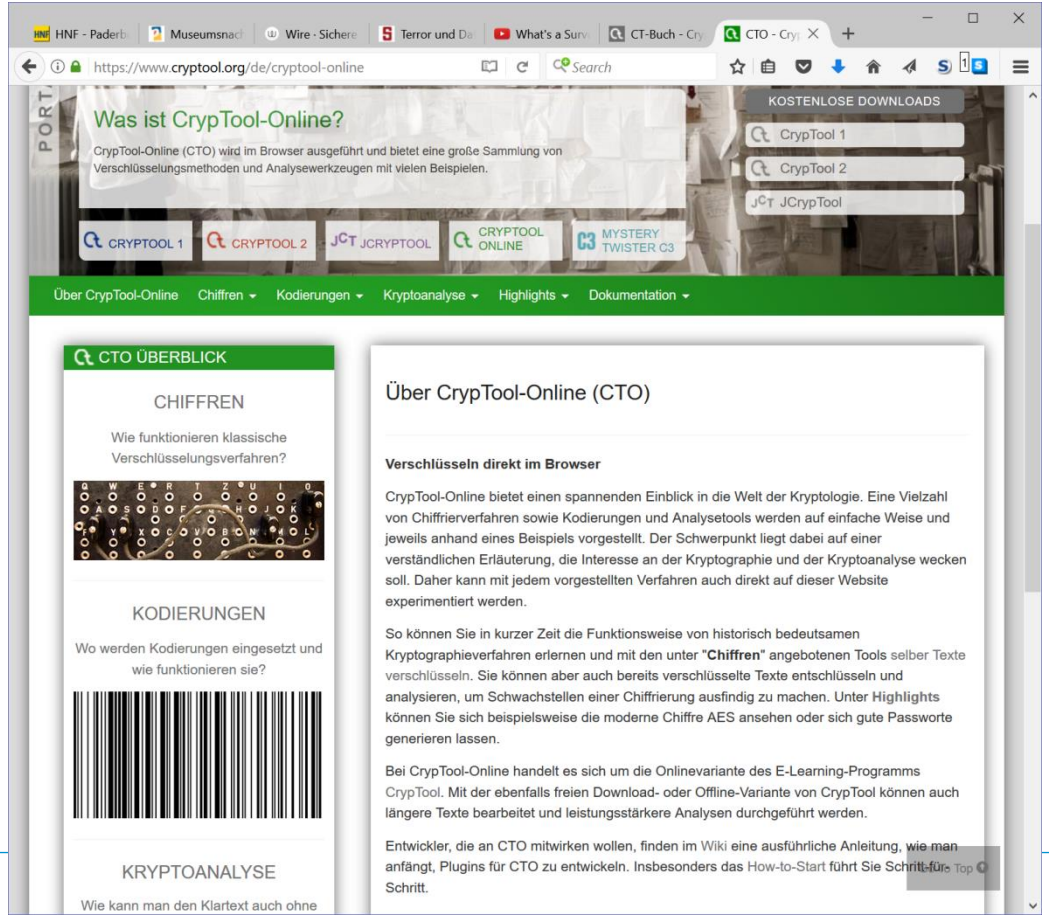
Screenshot zu Java-CrypTool: Auswahl an Verfahren + Visualisierungen (1)



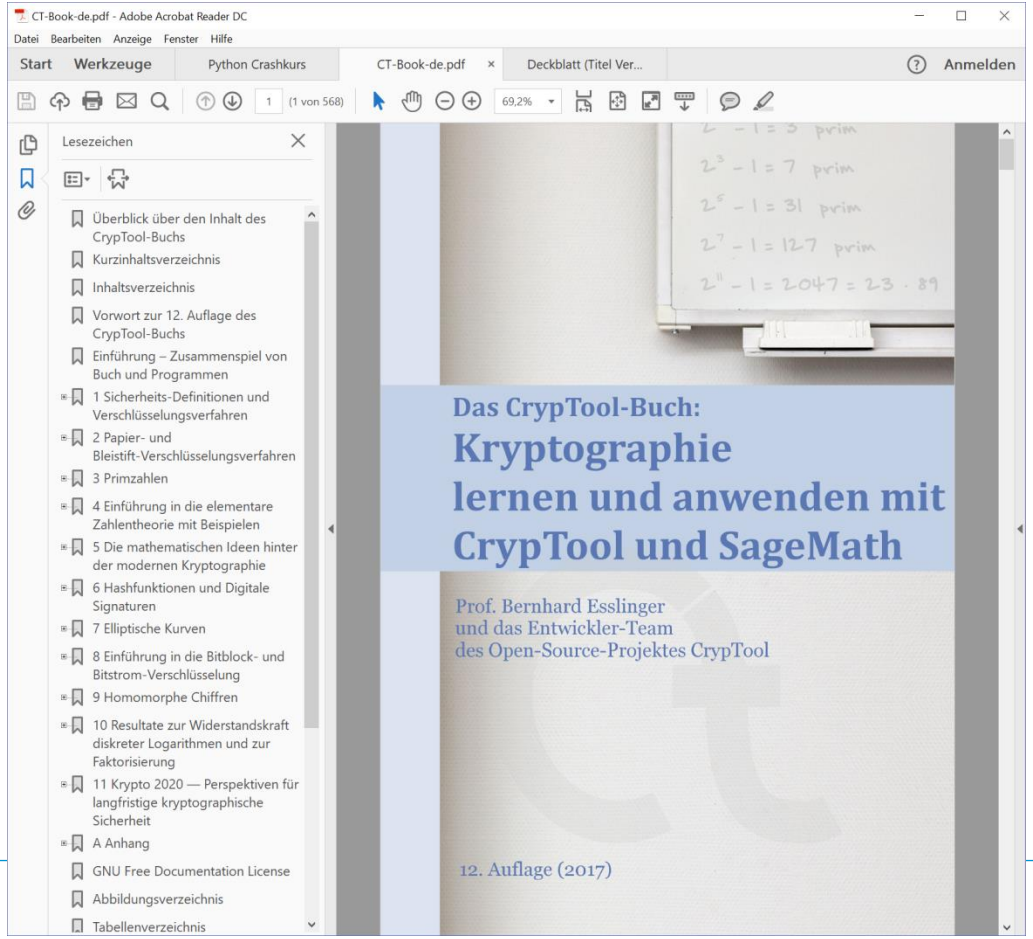
Screenshot zu Java-CrypTool: Auswahl an Verfahren + Visualisierungen (2)



Screenshot zu CrypTool-Online (für Browser und Smartphone):



Screenshot zu dem freien CrypTool-Buch: Kryptographie verstehen



Herunterladbar von:

https://www.cryptool.org/de/ctp-dokumentation/ctbuch

„Ich habe nichts zu verbergen“

- … Diese Aussage ist nicht wahr.
  Als rhetorische Frage wird oft vorwurfsvoll unterstellt, dass nur Verbrecher etwas zu verbergen haben.
- Jeder Mensch weiß Dinge über sich, die er als Teil seiner Privatsphäre für sich behalten möchte oder die er als Vertrauensperson sogar für sich behalten muss.
- Und wegen dieses Wunsches ist man noch lange kein Verbrecher.
- Geben Sie alle ihre Informationen und Passworte an andere? Glauben Sie, dass staatliche Organisationen nie gehackt werden und alle Mitarbeiter dort mit allen Informationen immer nur zweckgebunden umgehen?

Siehe Datenschutz-Statements beim http://zkm.de/event/2016/12/sicherheit-oder-datenschutz-ein-falscher-gegensatz