

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

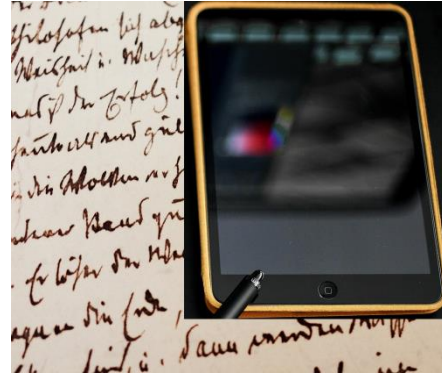
Briefträger



Provider

Internet

Provider



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

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

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

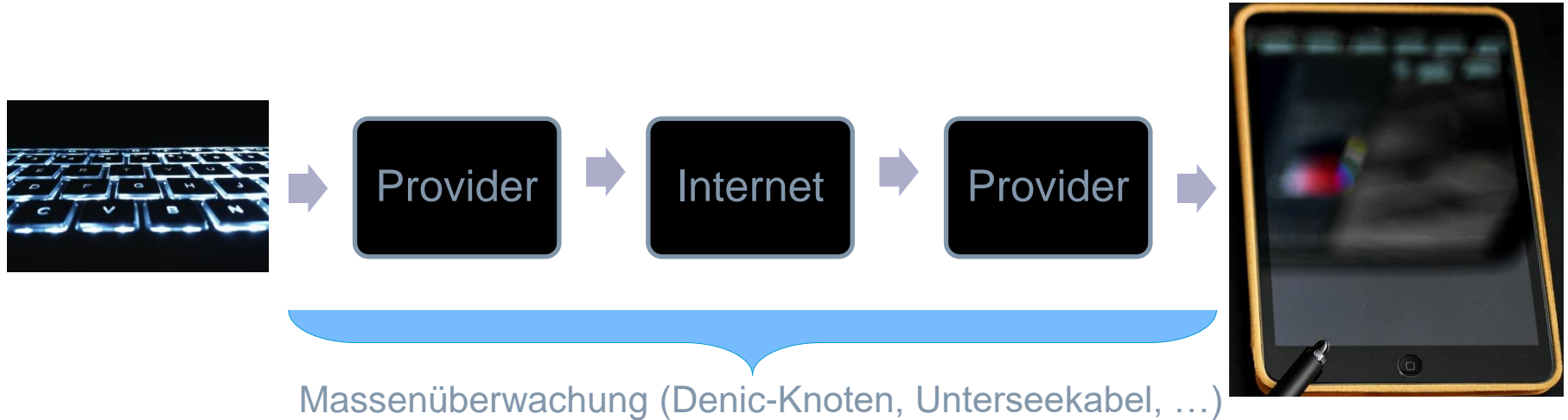
<http://www.emailtester.de/freemail/anbieter.php>

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.

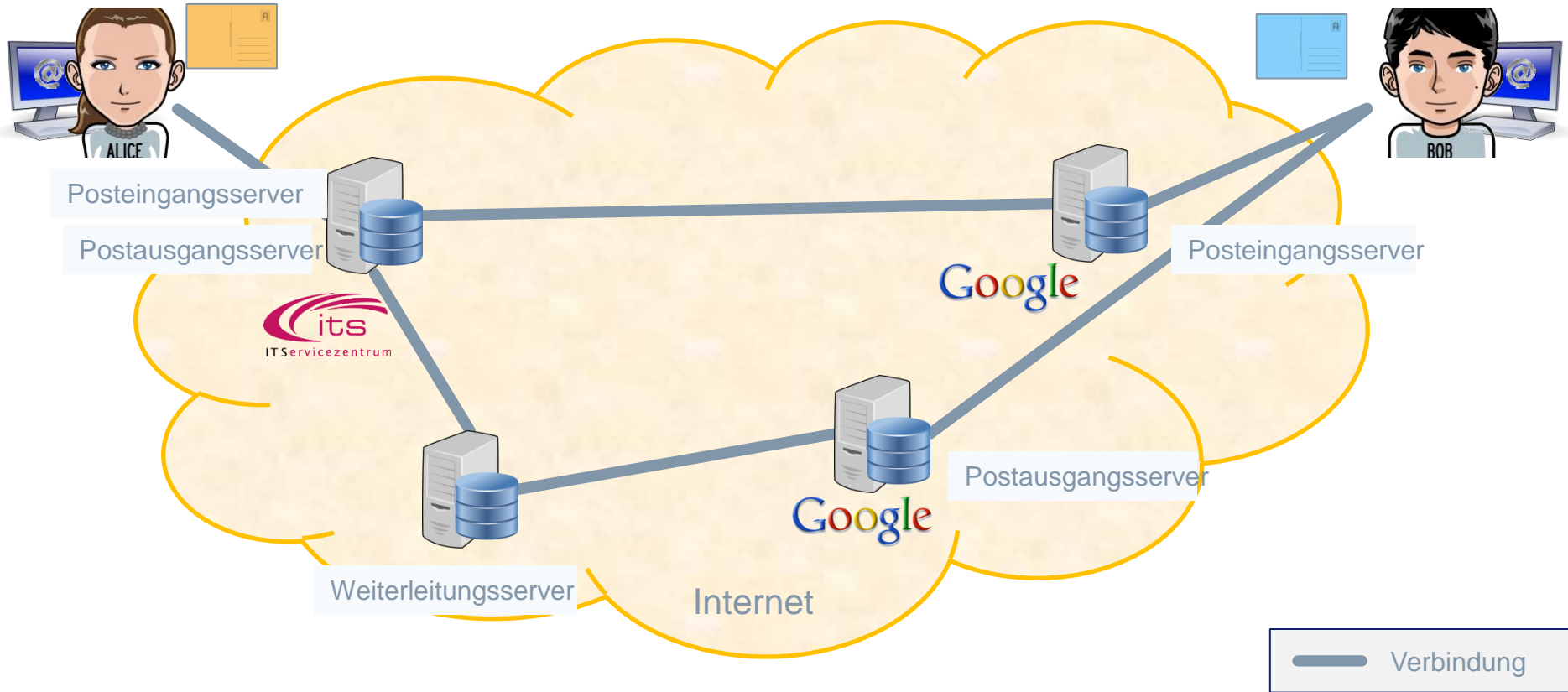
Wo kann Email abgehört werden?

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

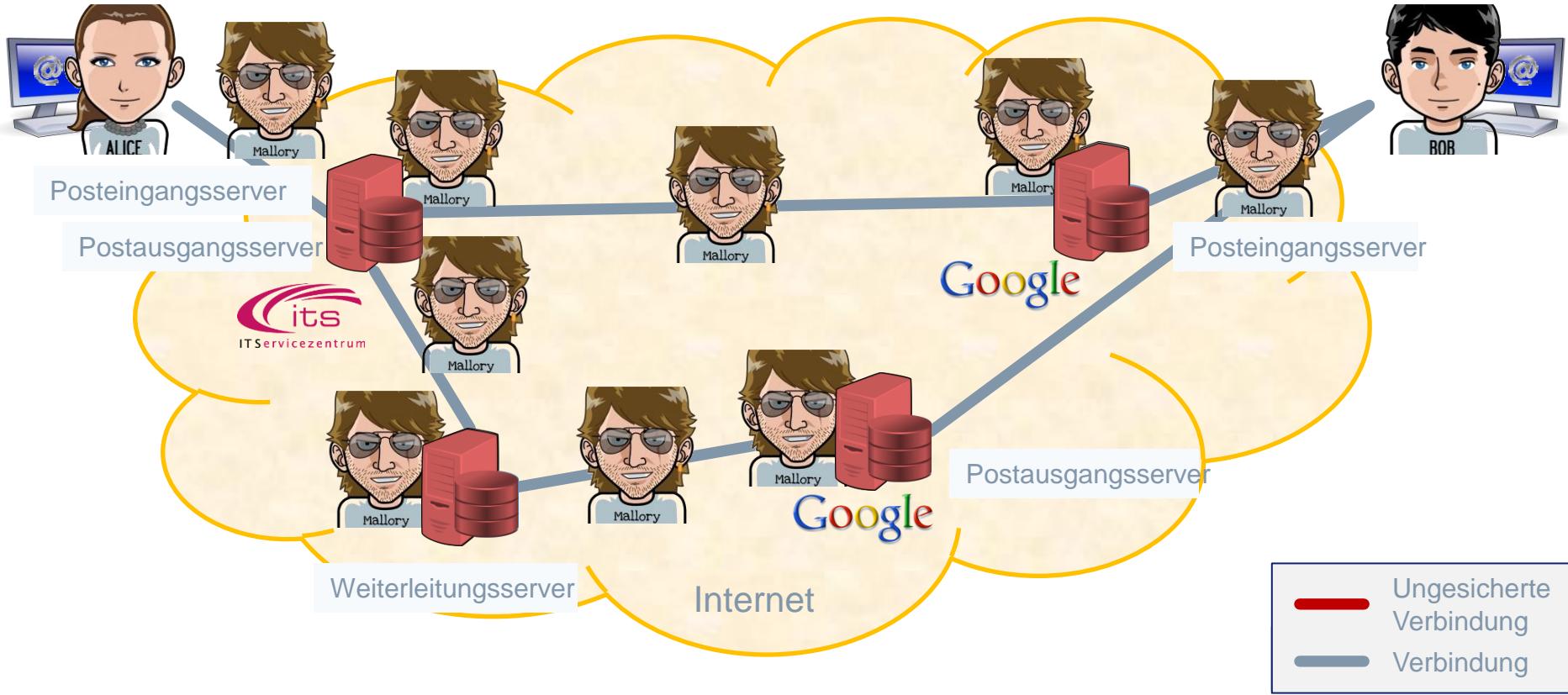


Abhörmöglichkeit: überall

Wie funktioniert E-Mail?



Wer kann meine E-Mail lesen?



	Ungesicherte Verbindung
	Verbindung

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

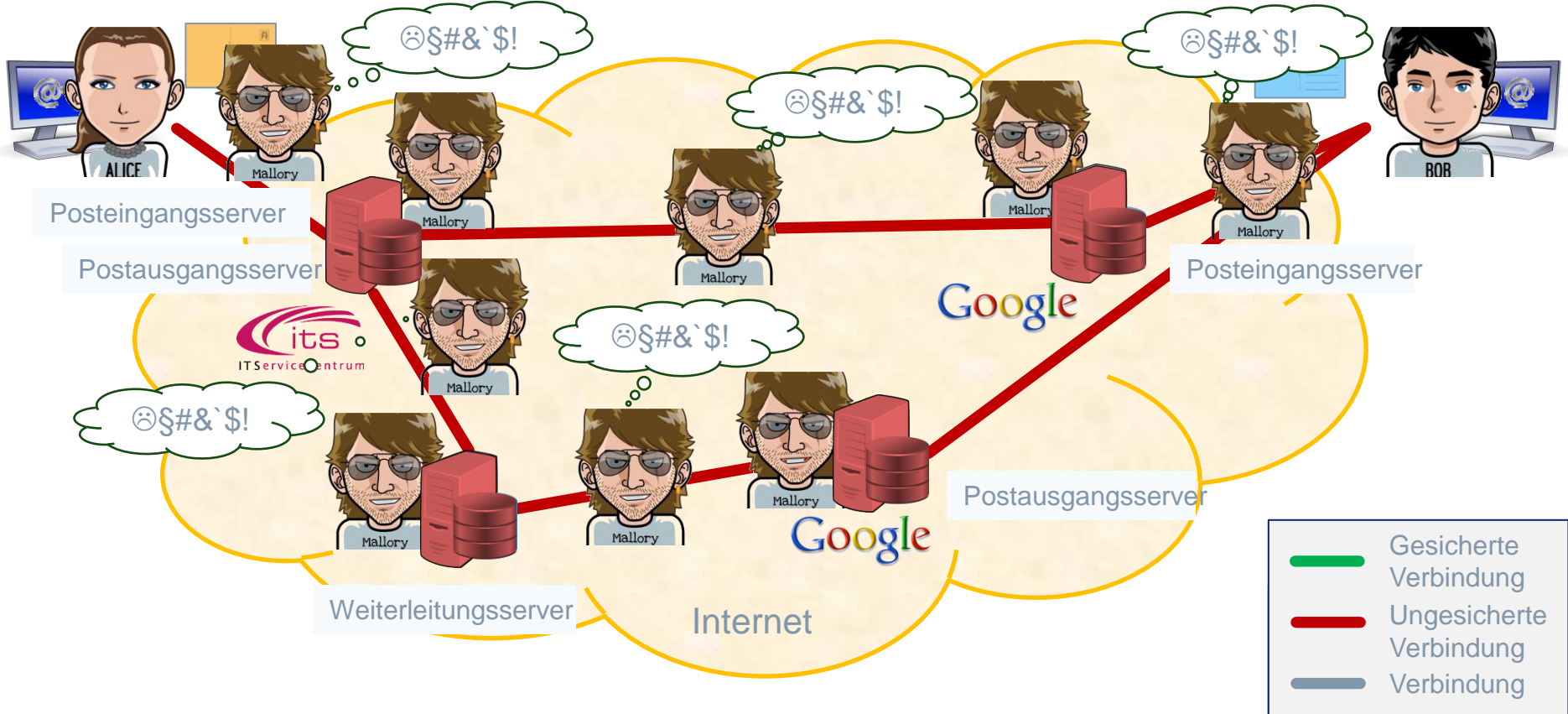
- Wird i.d.R. automatisch aktiviert, wenn von beiden Seiten unterstützt
- Bei Inkompatibilität wird stillschweigend die Sicherung abgeschaltet
- Benutzer hat keinen Einfluss darauf

Beispiele

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



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

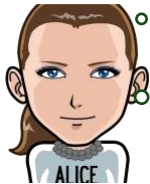
Unabhängig von der Sicherung des Transportweges

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.



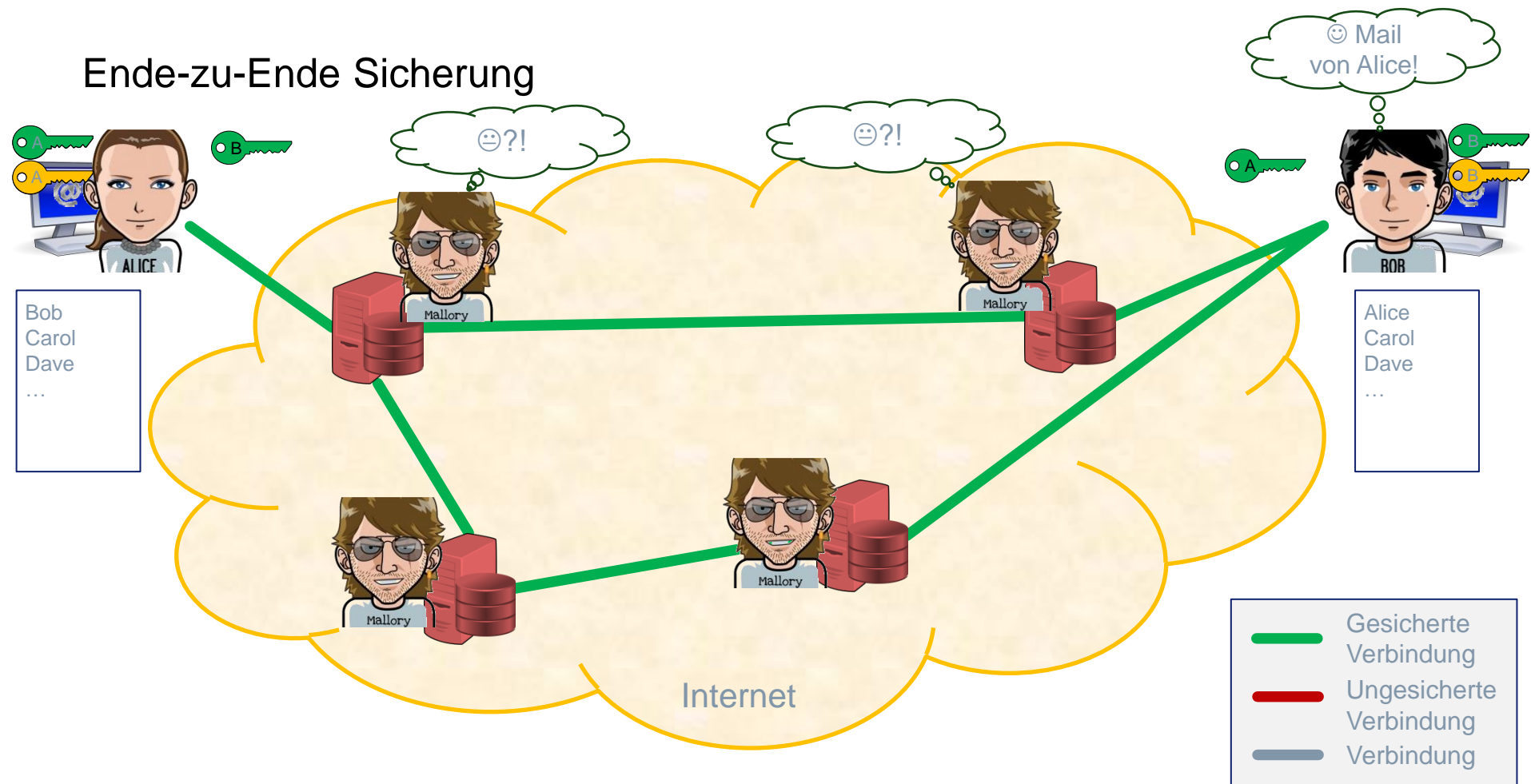
Nachricht

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



 **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

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 ???	[redacted]	15.08.2017 15:13

Von [redacted] ⭐

Betreff **Wissenschaftlicher Mitarbeiter**

An Mich <bernhard.esslinger@uni-siegen.de> ⭐

Antworten Weiterleiten Archivieren Junk Löschen Mehr

15.08.2017 06:46

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 20 Tagesplan

Awareness



Pixabay

Wirtschaftsspionage



„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 ...



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

CrypTool

- ❖ 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



Pixabay

From 5,32 € 

A Good American HD

from Friedrich Moser PRO on June 5, 2017



Rent €5.32

24-hour streaming period

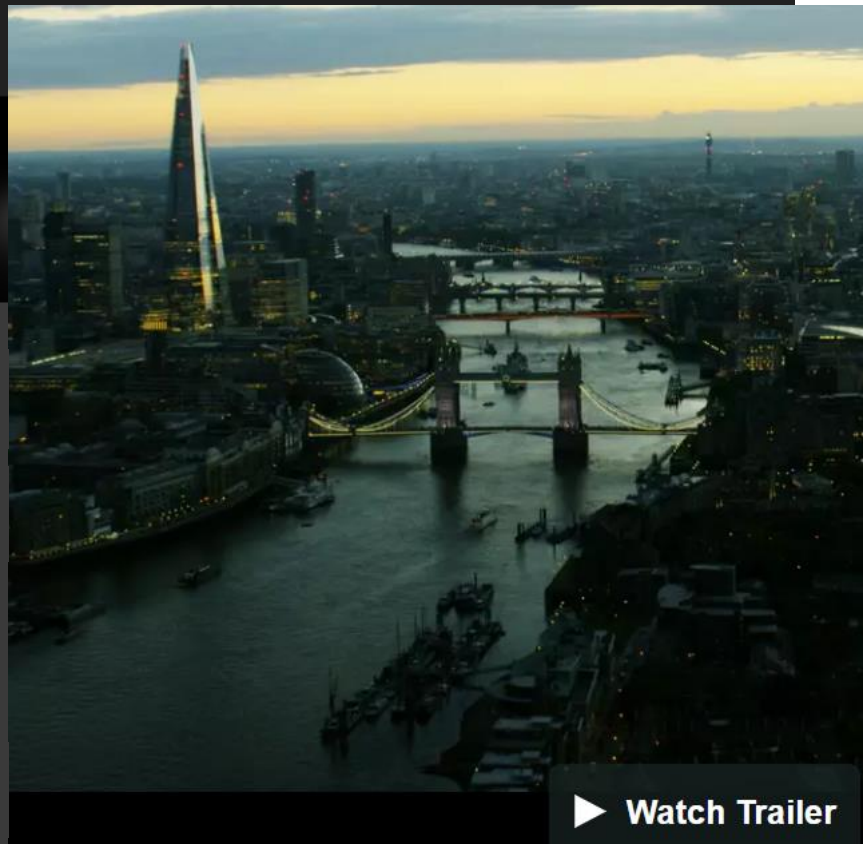
Terrorjagd im Netz

arte

SENDETERMINE

Dienstag, 12. September um 20.15 Uhr

Livestream: ja



▶ Watch Trailer

15
behörden-
bekannt

davon:

15 auf Terror-/Warnlisten

15 gewaltaffin

14 Islamistenkontakt



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.**

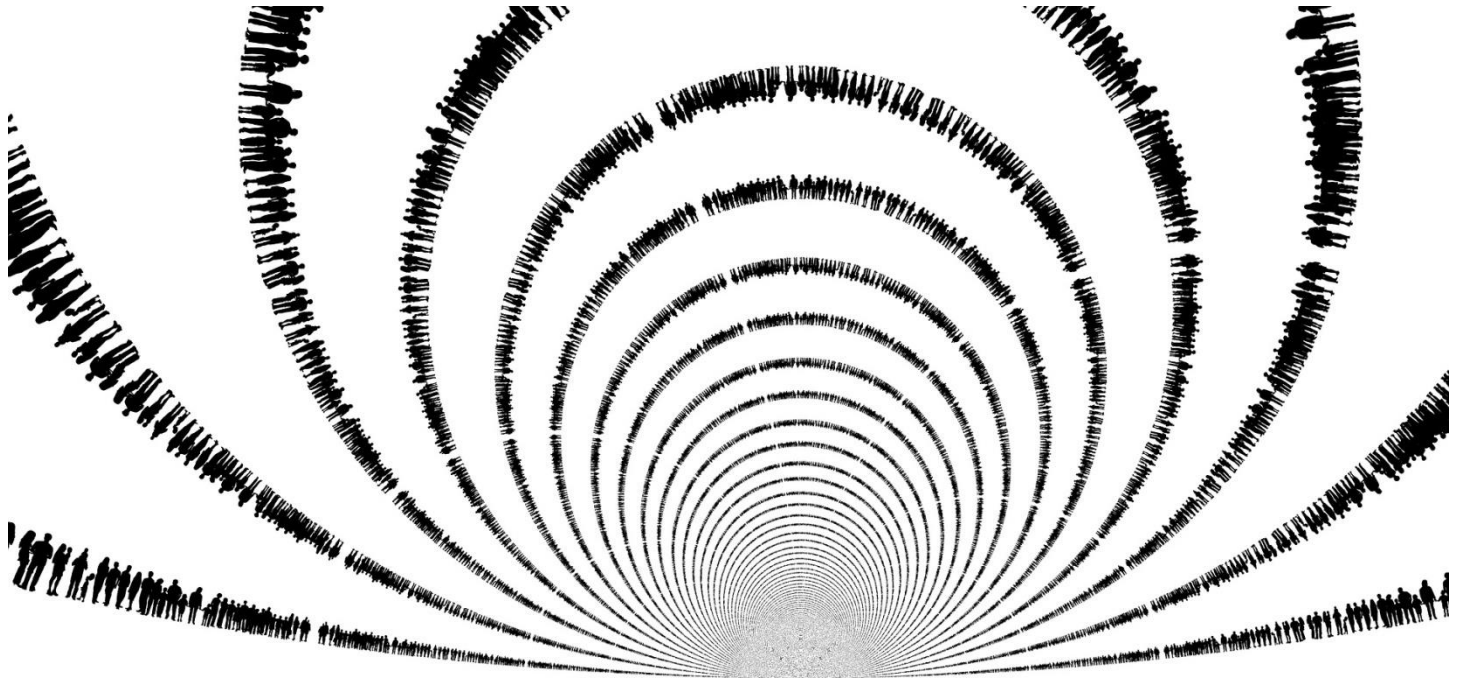
Ihr müsst ihn auf den Titelseiten führen.

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

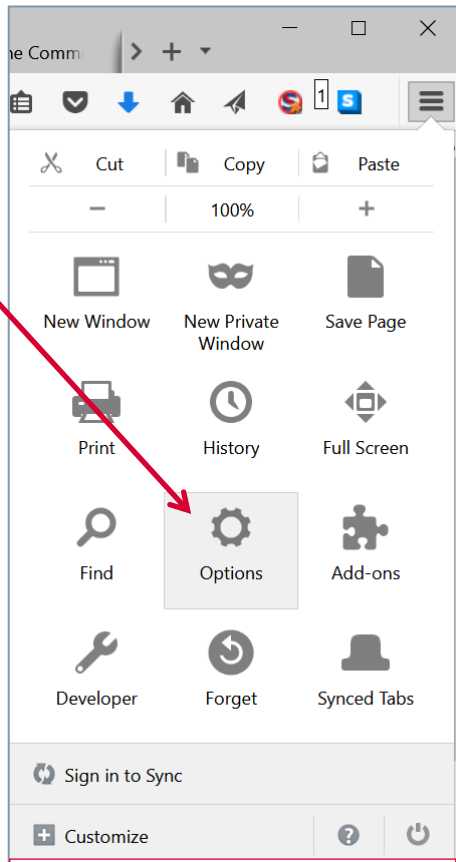
Ansehen

- <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=QtmjovN2Z0> Arte Doku: Überwachung Total, 1,5 h

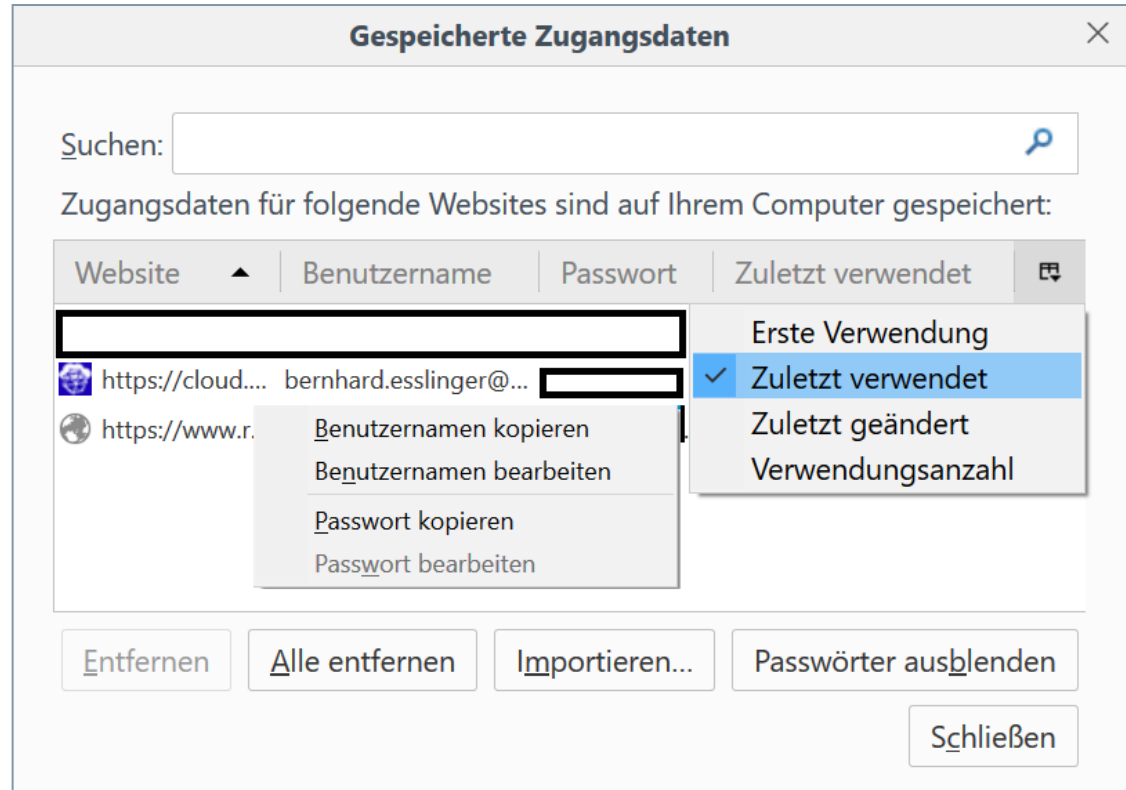
Aktiv werden,

- **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.**

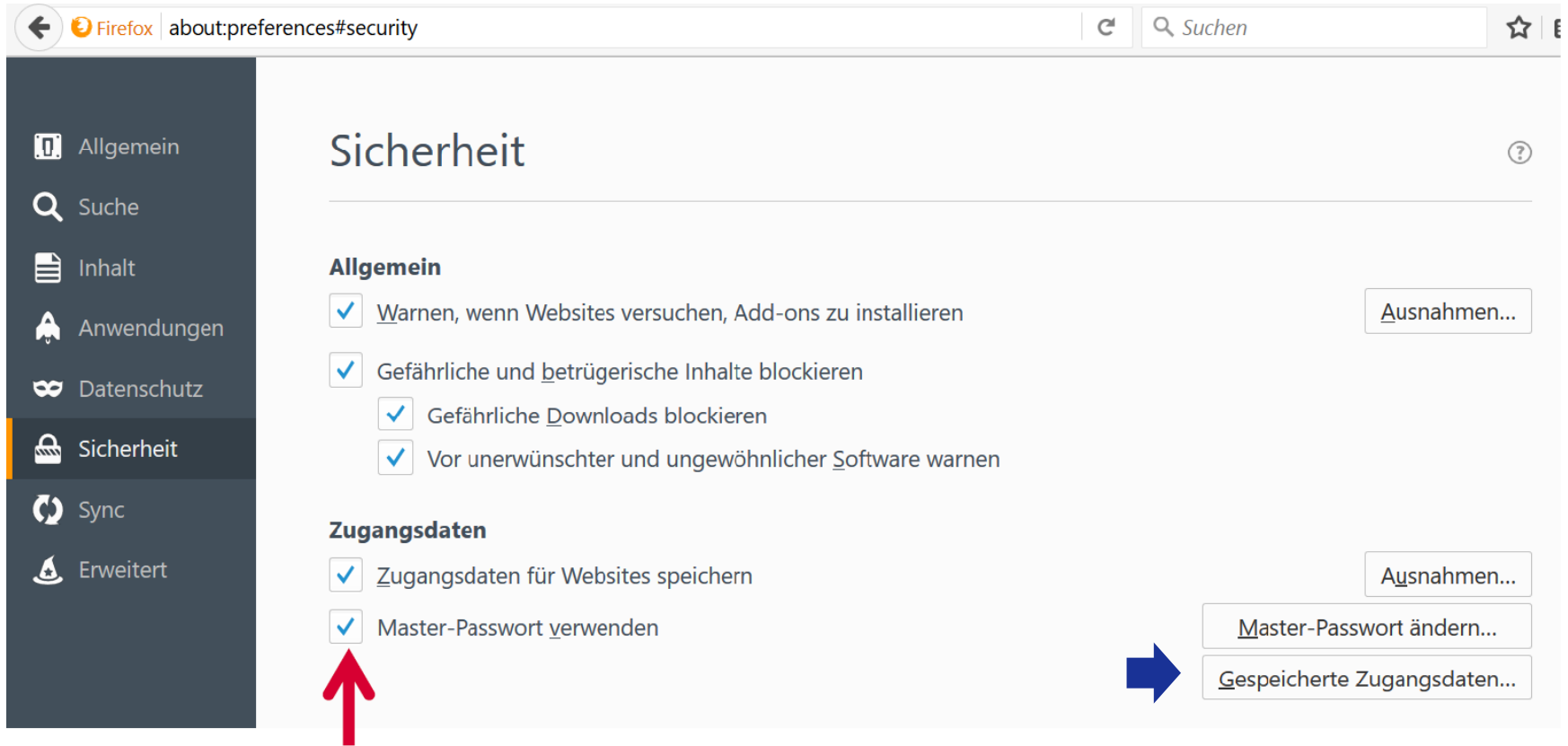
Nutzen Sie einen Passwortspeicher?



Firefox: Optionen,
Sicherheit,
Gespeicherte Logins



Jeder Passwort-Speicher braucht eine Zugangssicherung



The image shows the Firefox 'Security' settings page. The left sidebar has a blue arrow pointing to the 'Sicherheit' (Security) menu item. The main content area is titled 'Sicherheit' and contains two sections: 'Allgemein' and 'Zugangsdaten'. In the 'Allgemein' section, three options are checked: 'Warnen, wenn Websites versuchen, Add-ons zu installieren', 'Gefährliche und betrügerische Inhalte blockieren', and 'Vor unerwünschter und ungewöhnlicher Software warnen'. In the 'Zugangsdaten' section, two options are checked: 'Zugangsdaten für Websites speichern' and 'Master-Passwort verwenden'. A red arrow points to the 'Master-Passwort verwenden' checkbox. On the right side, there are buttons for 'Ausnahmen...', 'Master-Passwort ändern...', and 'Gespeicherte Zugangsdaten...'. A blue arrow points to the 'Gespeicherte Zugangsdaten...' button.

Firefox | about:preferences#security

Sicherheit

Allgemein

- Warnen, wenn Websites versuchen, Add-ons zu installieren [Ausnahmen...](#)
- Gefährliche und betrügerische Inhalte blockieren
 - Gefährliche Downloads blockieren
 - Vor unerwünschter und ungewöhnlicher Software warnen

Zugangsdaten

- Zugangsdaten für Websites speichern [Ausnahmen...](#)
- Master-Passwort verwenden [Master-Passwort ändern...](#)
[Gespeicherte Zugangsdaten...](#)

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)

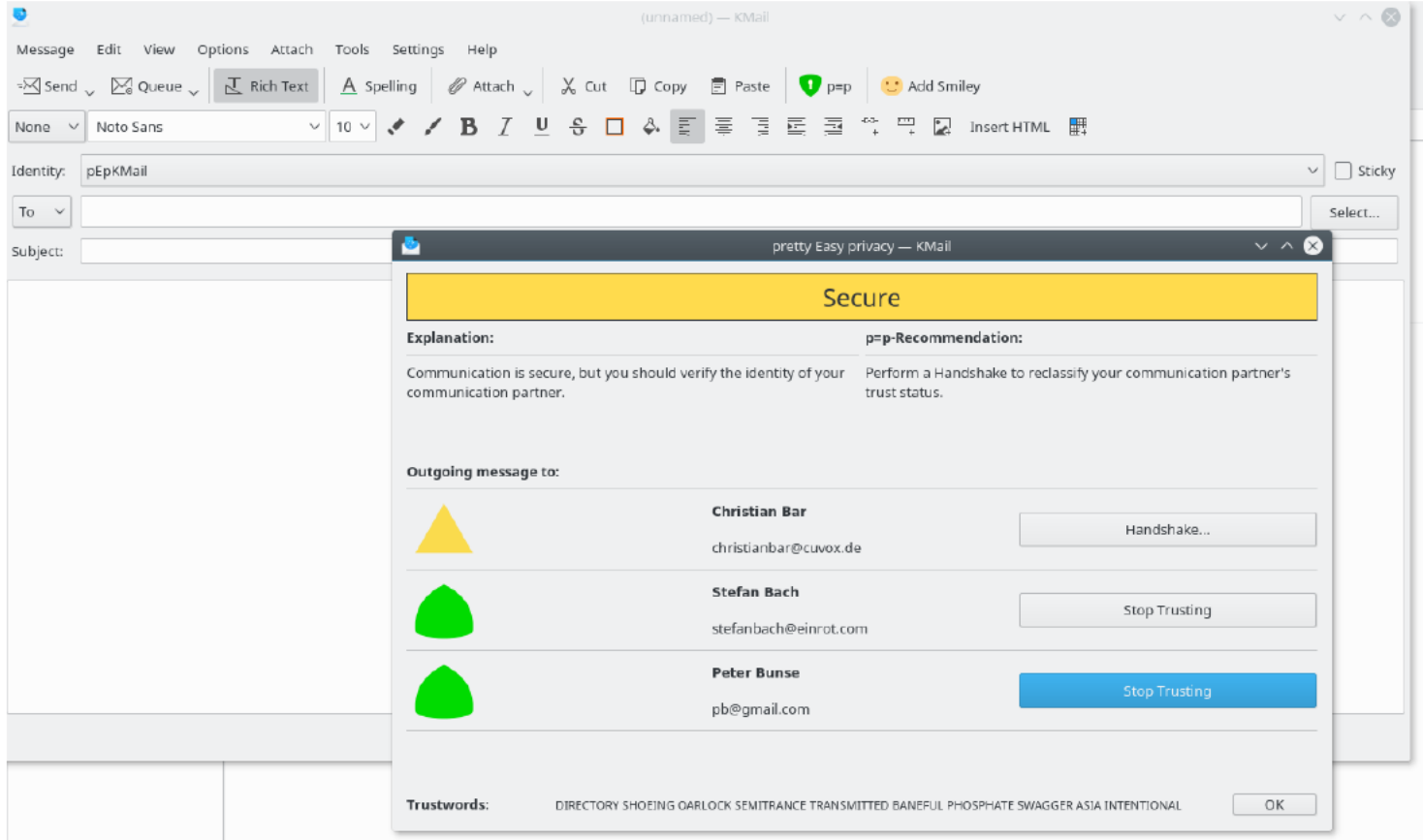
Nahtlose und **konfliktfreie Integration** der beiden Standards in alle E-Mail-Clients

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“.

Abbildung 11: Fertiger Prototyp von pEp in KMail

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



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

The screenshot displays the CrypTool 1.4.31 application window titled "startbeispiel-de.txt". The main interface is divided into several sections:

- File List:** Shows "startbeispiel-de.txt" selected.
- Main Text Area:** Contains instructions for using the tool and a Caesar cipher example. The example shows the plaintext "Tubsubctfjfm avs DszqUppm-Wfstjpotgbnjmjf 1-y (DU1)" being encrypted to "DszqUppm 1 (DU1) jtu fjo vngbohsjdift gsjft Mfsqzphsbnn av efo Uifnfo Lszquphsbqijf voe Lszqupbobmztf nju bvtgüismjdifs Pomjof-ljmgf voe nju wjmfno Wjtvbmjtjfsvohfö. Ejtjf Ufyuebufj ijmgju Jiofo cfj Jisfo fstufo Tdisjuufo nju DU1."
- Caesar Encryption Settings (Schlüssel eingabe: Caesar / ROT-13):**
 - Beschreibung:** Explains the Caesar cipher as a monoalphabetic substitution and mentions ROT-13 as a special case.
 - Variante auswählen:** Radio buttons for "Caesar" (selected) and "Rot-13".
 - Interpretation des ersten Alphabetzeichens:** Radio buttons for "Wert des ersten Alphabetzeichens = 0 (z.B. 'A'=0)" (selected) and "Wert des ersten Alphabetzeichens = 1 (z.B. 'A'=1)".
 - Schlüsseleingabe:** Radio buttons for "Alphabetzeichen" (selected) and "Zahlenwerte". A text box contains the value "1".
 - Informationen zur Verschlüsselung:** Shows "Verschiebung um 1" and "Das Alphabet (26 Zeichen) wird bei der Verschlüsselung abgebildet". It displays the alphabet mapping:
von: ABCDEFGHIJKLMNOPQRSTUVWXYZ
auf: BCDEFGHIJKLMNOPQRSTUVWXYZA
 - Buttons:** "Verschlüsseln", "Entschlüsseln", "Textoptionen", and "Abbrechen".
- Help Window (bottom left):** Titled "Caesar-Verschlüsselung von <startbeispiel-de.txt>, Schlüssel <B, KEY OF", it provides detailed instructions on how to use the tool's help system.

At the bottom of the application window, the status bar reads "Drücken Sie F1, um die Hilfe aufzurufen" and "Z:9 S:204 P:501".

Screenshot zu CrypTool 2: Beispiel zur automatischen Analyse

The screenshot displays the CrypTool 2.1 Monoalphabetic Substitution Analyzer interface. The main window is titled "Monoalphabetic Substitution Analyzer" and shows the following components:

- Input of the ciphertext:** A text area containing the ciphertext:


```
Mc gsaqxpsbqva b
twfmxwmpc gmqvh
mt b ohxvpl pl
hcgasqmpc fa dvmgv
wcmxt pl qnbmohzx
bsh shqnbghj dmxv
gmqvhshxzb bggspjnci
xp b shwmb tabho xvh
wcmxt oba fh tmcinh
nhooxst xvh optx
340 characters, 1 line
0 %
```
- Analysis Results:** A table showing the top 20 keys found during cryptanalysis:

#	Value	Attack	Key
0	18.59846	H	yanwbqcgdzflmopkrsyhvtjx
1	18.67282	H	ulqncedfkaobpanzsrhytk
2	18.76059	H	sodk/berncp/hm/tyzavugrvx
- Output of the plaintext:** A text area showing the decrypted plaintext:


```
incryptographyasubstitutionciph
erisamethodofencryptionbywhic
huntsforplaintextareplacedwith
hciphertextaccordingtoaregular
systemthemsuitmaybesingleletter
sthemostcommonpairsorletter
ripletsorlettersmixturesoftheabo
veandsoforththereceiverdeciphe
rsthetextbyperforminganinverse
substitution
285 characters, 1 line
0 %
```
- Output of the key:** A text area showing the key used for decryption:

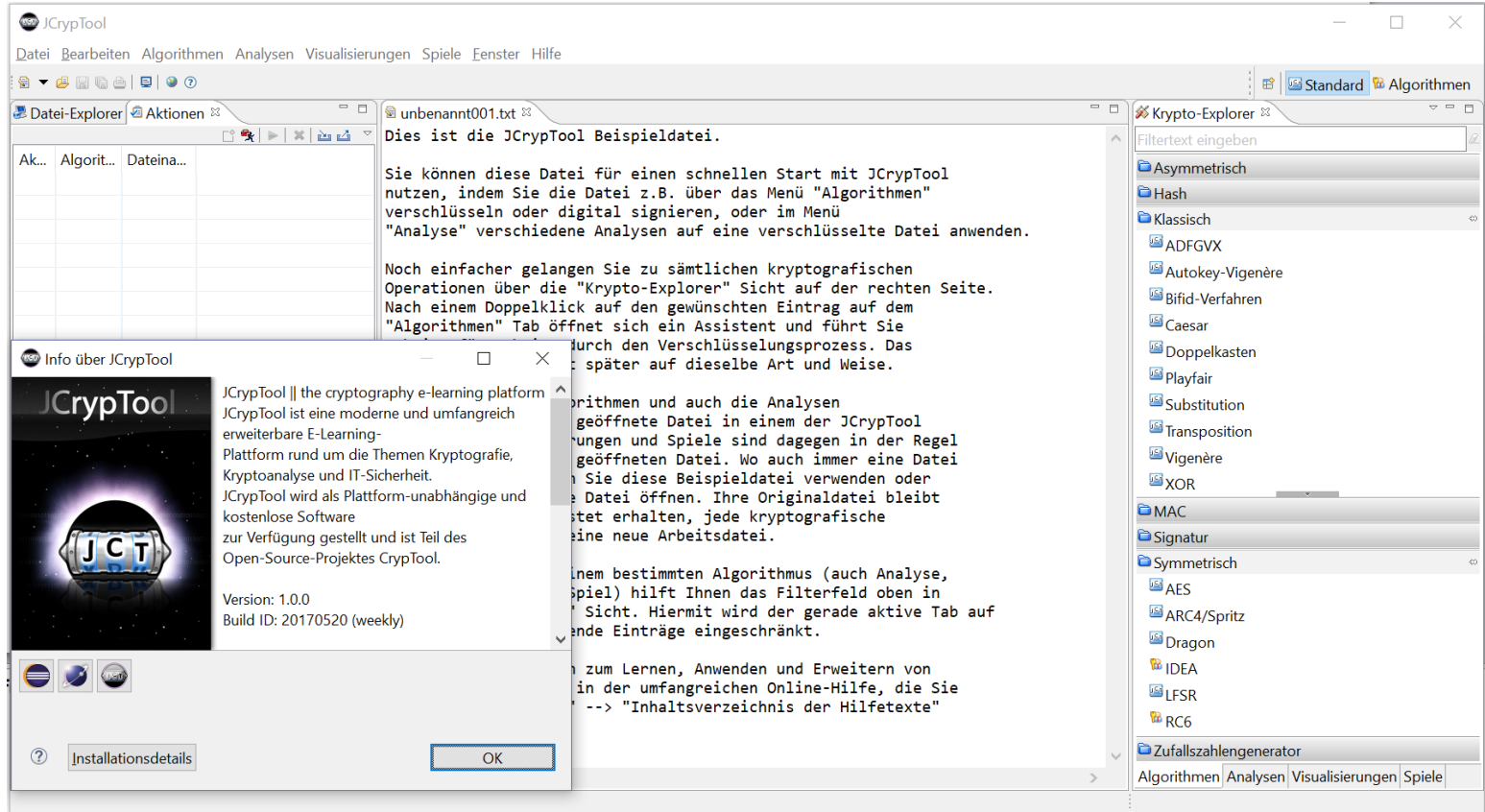

```
yanwbqcgdzflmopkrsyhvtjx
26 characters, 1 line
0 %
```

Below the main window, a text box explains the usage of the component:

This template demonstrates the usage of the component Monoalphabetic Substitution Analyzer.

The presentation of the analyzer component is split in an upper part that displays the start, elapsed, and end time as well as a table in the lower part to show the best 20 keys that have been found during the cryptanalysis. This table shows for each found key a rank (column 1 "#"), the value of the cost function (column 2 "Value"), the attack which found the key (column 3 "Attack"), the key itself (column 4 "Key"), and the according plaintext (column 5 "Text"). The value of the cost function is the logarithm of the arithmetic mean n-gram probabilities that are contained in the according plaintext. The difference of this value between two keys determines the range of how much one key is better than the other. In column 3 ("Attack") the attack method which found the key is displayed. A "G" stands for the genetic attack and a "D" stands for the dictionary attack. On double click on a row the according plaintext and the according key is forwarded to the outputs. Furthermore, the best plaintext and key currently found are outputted automatically.

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



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

The screenshot displays the Java-CrypTool application window. The menu bar includes 'Datei', 'Bearbeiten', 'Algorithmen', 'Analysen', 'Visualisierungen', 'Spiele', 'Fenster', and 'Hilfe'. The 'Visualisierungen' menu is open, listing various cryptographic techniques. A blue arrow points to 'Huffman-Kodierung'. Below the menu, two probability trees are visible. The left tree shows a Huffman tree for the text 'NL t j >', with root probability 8,748% and leaf probabilities for 'N', 'L', 't', 'j', and '>'. The right tree shows a Huffman tree for the text 'H I J O B C', with root probability 100% and leaf probabilities for 'H', 'I', 'J', 'O', 'B', and 'C'. The interface also shows a toolbar with 'Standard' and 'Algorithmen' buttons, and a text area with instructions: 'Klicken Sie auf eines der Blätter und man kann den Zweig bei Bedarf ver...'.

- Ameisenkolonie-Optimierung
- Android-Mustersperre (AUP)
- ARC4 / Spritz
- Chinesischer Restsatz
- Differential Power Analysis / Double and Add
- Diffie-Hellman Schlüsselaustausch (EC)
- ElGamal-Kryptosystem
- Elliptische Kurven Berechnungen
- Erweiterter Euklid / Wechselwegnahme
- Erweitertes RSA-Kryptosystem
- Feige Fiat Shamir
- Fiat Shamir
- Graphenisomorphie
- Grille
- Hash-Sensitivität
- Homomorphe Verschlüsselung
- Huffman-Kodierung
- Innere Zustände im Data Encryption Standard (DES)
- Kleptographie
- Magische Tür
- Merkle-Hellman Rucksack-Verschlüsselung
- MerkleTree-Signaturen
- Multipartite Key Exchange
- Public-Key-Infrastruktur
- RSA-Kryptosystem
- Shamir's Secret Sharing
- Shanks Babystep-Giantstep
- Signatur-Demo
- Signatur-Verifikation

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

Was ist CrypTool-Online?

CrypTool-Online (CTO) wird im Browser ausgeführt und bietet eine große Sammlung von Verschlüsselungsmethoden und Analysewerkzeugen mit vielen Beispielen.

KOSTENLOSE DOWNLOADS


- CrypTool 1
- CrypTool 2
- JCrypTool

Über CrypTool-Online | Chiffren | Kodierungen | Kryptoanalyse | Highlights | Dokumentation

CTO ÜBERBLICK


CHIFFREN

Wie funktionieren klassische Verschlüsselungsverfahren?



KODIERUNGEN

Wo werden Kodierungen eingesetzt und wie funktionieren sie?



KRYPTOANALYSE

Wie kann man den Klartext auch ohne

Über CrypTool-Online (CTO)

Verschlüsseln direkt im Browser

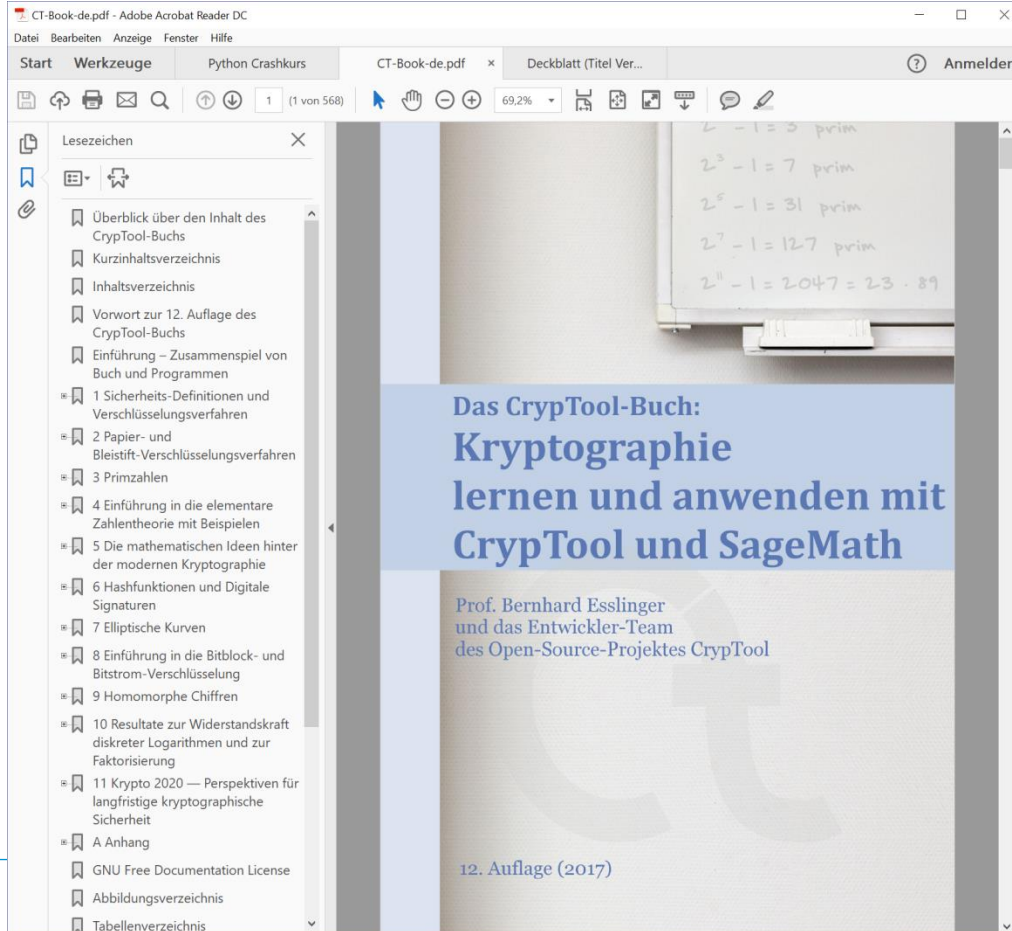
CrypTool-Online bietet einen spannenden Einblick in die Welt der Kryptologie. Eine Vielzahl von Chiffrierverfahren sowie Kodierungen und Analysetools werden auf einfache Weise und jeweils anhand eines Beispiels vorgestellt. Der Schwerpunkt liegt dabei auf einer verständlichen Erläuterung, die Interesse an der Kryptographie und der Kryptoanalyse wecken soll. Daher kann mit jedem vorgestellten Verfahren auch direkt auf dieser Website experimentiert werden.

So können Sie in kurzer Zeit die Funktionsweise von historisch bedeutsamen Kryptographieverfahren erlernen und mit den unter "**Chiffren**" angebotenen Tools selber Texte verschlüsseln. Sie können aber auch bereits verschlüsselte Texte entschlüsseln und analysieren, um Schwachstellen einer Chiffrierung ausfindig zu machen. Unter Highlights können Sie sich beispielsweise die moderne Chiffre AES ansehen oder sich gute Passworte generieren lassen.

Bei CrypTool-Online handelt es sich um die Onlinevariante des E-Learning-Programms CrypTool. Mit der ebenfalls freien Download- oder Offline-Variante von CrypTool können auch längere Texte bearbeitet und leistungsstärkere Analysen durchgeführt werden.

Entwickler, die an CTO mitwirken wollen, finden im Wiki eine ausführliche Anleitung, wie man anfängt, Plugins für CTO zu entwickeln. Insbesondere das How-to-Start führt Sie Schritt-für-Schritt.

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>