



Joschka Heinrich¹



Carsten Knoll²

Sichere Kommunikation: Warum & Wie

KRETA – Oktober 2017

FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)

FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
 - ▶ *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrenden Summen von Zeitschriften-Verlagen gekauft werden müssen

FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
 - ▶ *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrenden Summen von Zeitschriften-Verlagen gekauft werden müssen
- ▶ Bisherige Projekte
 - ▶ Linux-Install-Party, Linux-Presentation-Day
 - ▶ Monatliche Sprechstunde zu L^AT_EX u.a.
 - ▶ Programmpapier
 - ▶ „Uni-Stick“: 80 × 8 GB mit freier Software
 - ▶ Verschlüsselungsgewinnspiel

FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
 - ▶ *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrenden Summen von Zeitschriften-Verlagen gekauft werden müssen
- ▶ Bisherige Projekte
 - ▶ Linux-Install-Party, Linux-Presentation-Day
 - ▶ Monatliche Sprechstunde zu L^AT_EX u.a.
 - ▶ Programmpapier
 - ▶ „**Uni-Stick**“: **80 × 8 GB mit freier Software**
 - ▶ Verschlüsselungsgewinnspiel



FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
 - ▶ *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrenden Summen von Zeitschriften-Verlagen gekauft werden müssen
- ▶ Bisherige Projekte
 - ▶ Linux-Install-Party, Linux-Presentation-Day
 - ▶ Monatliche Sprechstunde zu \LaTeX u.a.
 - ▶ Programmpapier
 - ▶ **„Uni-Stick“: 80 × 8 GB mit freier Software**
 - ▶ Verschlüsselungsgewinnspiel



FSFW – Freie Software und Freies Wissen

- ▶ Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, ...)
- ▶ Warum machen wir das? Aus Überzeugung!
 - ▶ *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
 - ▶ *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrenden Summen von Zeitschriften-Verlagen gekauft werden müssen
- ▶ Bisherige Projekte
 - ▶ Linux-Install-Party, Linux-Presentation-Day
 - ▶ Monatliche Sprechstunde zu L^AT_EX u.a.
 - ▶ Programmpapier
 - ▶ „Uni-Stick“: 80 × 8 GB mit freier Software
 - ▶ Verschlüsselungsgewinnspiel
- ▶ Für (Mitmachen-)Interessierte: <https://fsfw-dresden.de>



Ablauf

1) Verschlüsselung in der Theorie

- ▶ Diskussion: „Ich habe doch nichts zu verbergen“
- ▶ Schutzziele sicherer Kommunikation
- ▶ Funktionsweise PGP

Ablauf

1) Verschlüsselung in der Theorie

- ▶ Diskussion: „Ich habe doch nichts zu verbergen“
- ▶ Schutzziele sicherer Kommunikation
- ▶ Funktionsweise PGP

2) PGP in der Praxis

- ▶ Installation (individuell)
- ▶ Schlüsselgenerierung
- ▶ E-Mails verschlüsseln
- ▶ Ausblick

Diskussion: „Ich habe doch nichts zu verbergen“

→ 10 Minuten freie Diskussion

- ▶ je 2-5 Personen
- ▶ möglichst viele verschiedene Perspektiven einnehmen (Bürger*in, Bürgerrechtler*in, Innenminister*in, Freiheitskämpfer*in, ...)
- ▶ Argumente sammeln

Diskussion: „Ich habe doch nichts zu verbergen“

→ 10 Minuten freie Diskussion

- ▶ je 2-5 Personen
- ▶ möglichst viele verschiedene Perspektiven einnehmen (Bürger*in, Bürgerrechtler*in, Innenminister*in, Freiheitskämpfer*in, ...)
- ▶ Argumente sammeln
- ▶ Stichworte
 - ▶ Kriminalität (Einbruch, Erpressung, ...)
 - ▶ Privatsphäre
 - ▶ Selbstzensur (analog: Kamera-Attrappen)
 - ▶ Demokratie
 - ▶ Journalismus
 - ▶ Whistleblowing
 - ▶ Erstarren totalitärer Strukturen

„Ich habe doch nichts zu verbergen“

- ▶ In Menschheitsgeschichte:
viele Beispiele für **rücksichtslosen Egoismus**
 - ▶ „Wissen ist Macht“
- ⇒ sensibler Umgang mit Informationen empfehlenswert

„Ich habe doch nichts zu verbergen“

- ▶ In Menschheitsgeschichte:
viele Beispiele für **rücksichtslosen Egoismus**
 - ▶ „Wissen ist Macht“
- ⇒ sensibler Umgang mit Informationen empfehlenswert
- ▶ **Digitalisierung verstärkt das Problem**
 - ▶ E-Mail¹ ist wie Postkarte: unterwegs² lesbar
 - ▶ E-Mail ist noch schlimmer als Postkarte:
 - ▶ automatisiert auswertbar
 - ▶ unbemerkt kopierbar
 - ▶ unbemerkt veränderbar (inkl. Metadaten, bspw. Absender)

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**

→ A weiß, nur B kann Nachricht lesen

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**

 - A weiß, nur B kann Nachricht lesen

- **Integrität**

 - B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**

 - A weiß, nur B kann Nachricht lesen

- **Integrität**

 - B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden

- **Anonymität**

 - A bestimmt, wem eigene Identität preisgegeben wird

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
→ A weiß, nur B kann Nachricht lesen
- **Integrität**
→ B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden
- **Anonymität**
→ A bestimmt, wem eigene Identität preisgegeben wird
- **Verfügbarkeit**
→ obige Schutzziele werden in annehmbarer Zeit realisiert

PGP – Begriffe

- ▶ asymmetrische Verschlüsselung
- ▶ Privater Schlüssel (*private key*)
- ▶ Öffentlicher Schlüssel (*public key*)
- ▶ GPG vs. PGP

PGP – Begriffe

- ▶ asymmetrische Verschlüsselung
- ▶ Privater Schlüssel (*private key*)
- ▶ Öffentlicher Schlüssel (*public key*)
- ▶ GPG vs. PGP
- ▶ Schlüsselservers (*keyserver*)
- ▶ Fingerabdruck
- ▶ Metadaten
- ▶ Widerrufszeugnis

PGP – Das Problem

- ▶ *P1*: A möchte Nachricht an B vertraulich schicken
- ⇒ Nachricht verschlüsseln

PGP – Das Problem

- ▶ *P1*: A möchte Nachricht an B vertraulich schicken
- ⇒ Nachricht verschlüsseln
- ▶ *P2*: Schlüsselverteilung
- ⇒ asymmetrisches Verschlüsselungsverfahren (PGP)
 - ▶ Es gibt: **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel

PGP – Das Problem

- ▶ *P1*: A möchte Nachricht an B vertraulich schicken
- ⇒ Nachricht verschlüsseln
- ▶ *P2*: Schlüsselverteilung
- ⇒ asymmetrisches Verschlüsselungsverfahren (PGP)
 - ▶ Es gibt: **öffentlicher Schlüssel** und **privater Schlüssel**
 - ▶ **ÖS**: zum Verschlüsseln



- ▶ **PS**: zum Entschlüsseln



PGP – Das Problem

- ▶ *P1*: A möchte Nachricht an B vertraulich schicken
- ⇒ Nachricht verschlüsseln
- ▶ *P2*: Schlüsselverteilung
- ⇒ asymmetrisches Verschlüsselungsverfahren (PGP)
 - ▶ Es gibt: **öffentlicher Schlüssel** und **privater Schlüssel**
 - ▶ **ÖS**: zum Verschlüsseln



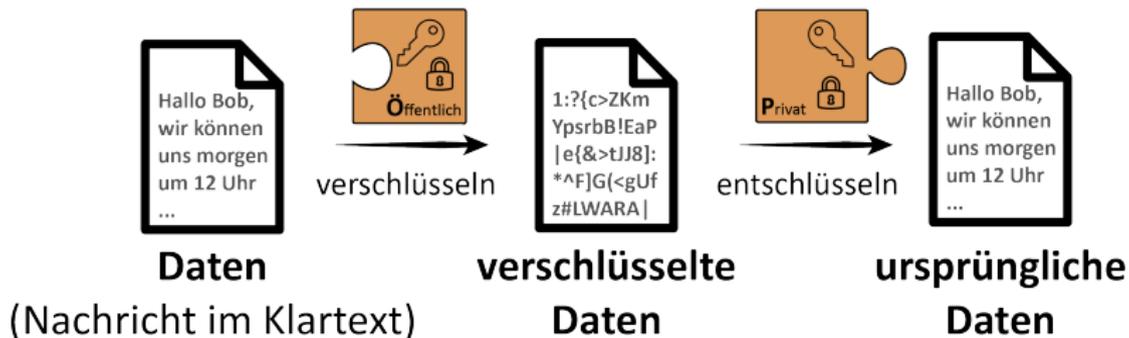
- ▶ **PS**: zum Entschlüsseln



Oft eingesetzte, freie Implementierung: GPG (**G**NU **P**rivacy **G**uard, 1999)

Nicht freier Vorläufer & Namensgeber des Verfahrens: PGP (**P**retty **G**ood **P**rivacy, 1991)

PGP – Funktionsweise 1



PGP – Funktionsweise 2

- ▶ Öffentlicher Schlüssel („public key“)
 - ▶ Benötigt zum Verschlüsseln
 - ▶ Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
 - ▶ kann/sollte man weitergeben → auf Keyserver hochladen

Bsp: <http://pgp.mit.edu> zu bedenken: nicht löschar, nur widerrufbar ⇒ Anonymität gefährdet

PGP – Funktionsweise 2

- ▶ Öffentlicher Schlüssel („public key“)
 - ▶ Benötigt zum Verschlüsseln
 - ▶ Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
 - ▶ kann/sollte man weitergeben → auf Keyserver hochladen

Bsp: <http://pgp.mit.edu> zu bedenken: nicht löschar, nur widerrufbar ⇒ Anonymität gefährdet

- ▶ Privater Schlüssel („private key“)
 - ▶ Benötigt zum Entschlüsseln
 - ▶ Darf nicht verloren gehen
 - Entschlüsseln wäre dann unmöglich
 - ▶ Darf nicht in fremde Hände kommen
 - andere können meine Mails entschlüsseln
 - ▶ Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

PGP – Funktionsweise 2

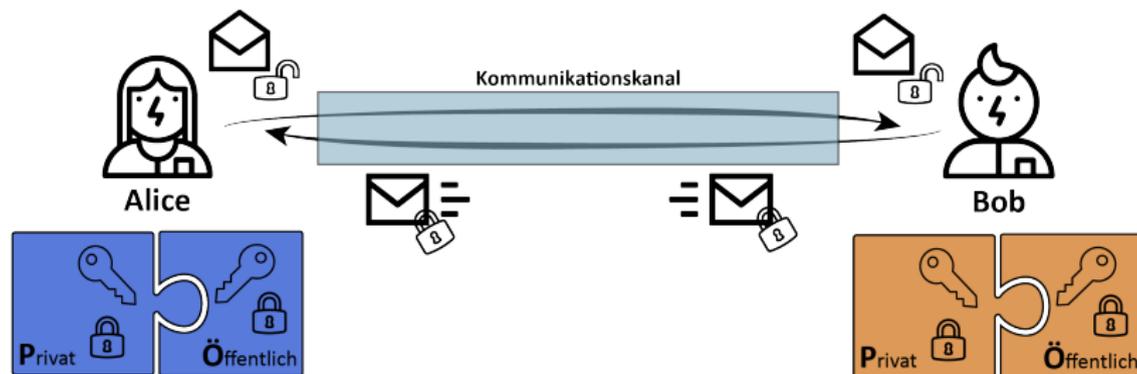
- ▶ Öffentlicher Schlüssel („public key“)
 - ▶ Benötigt zum Verschlüsseln
 - ▶ Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
 - ▶ kann/sollte man weitergeben → auf Keyserver hochladen

Bsp: <http://pgp.mit.edu> zu bedenken: nicht löschar, nur widerrufbar ⇒ Anonymität gefährdet

- ▶ Privater Schlüssel („private key“)
 - ▶ Benötigt zum Entschlüsseln
 - ▶ Darf nicht verloren gehen
 - Entschlüsseln wäre dann unmöglich
 - ▶ Darf nicht in fremde Hände kommen
 - andere können meine Mails entschlüsseln
 - ▶ Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

⇒ Sicheres Backup wichtig

PGP – Funktionsweise 3



Praxisteil – Installation 1

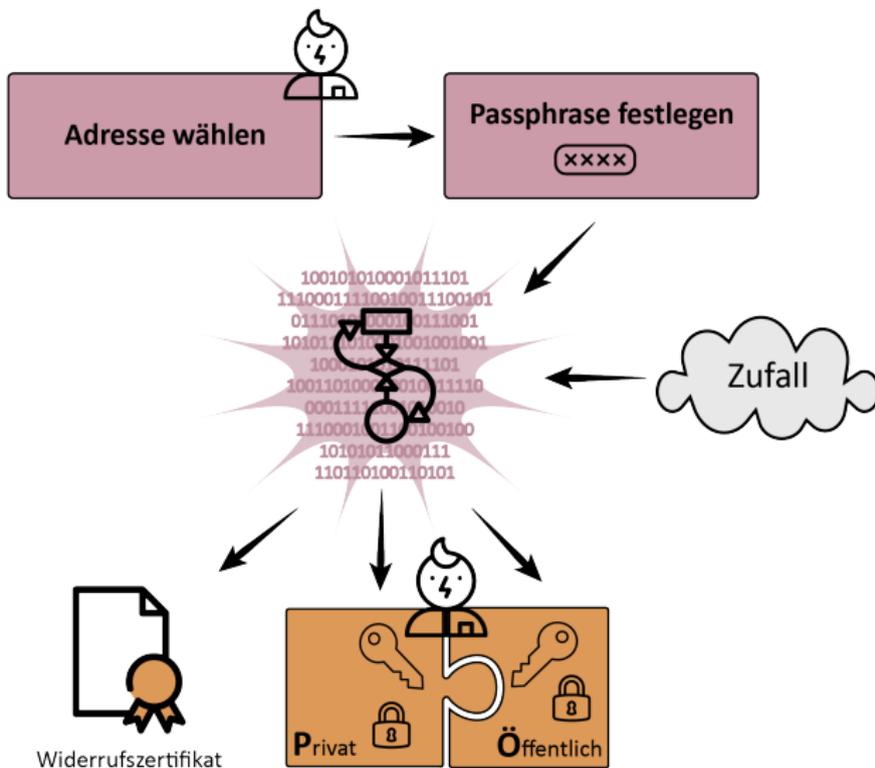


- ▶ Anleitungen: <https://fsfw-dresden.de/gpg>

Praxisteil – Installation 2

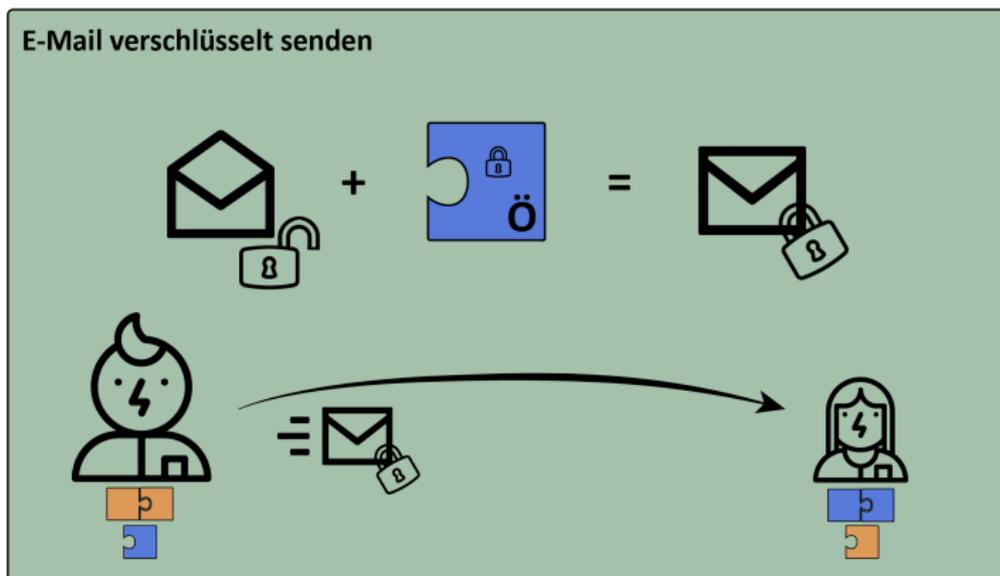
- ▶ Anleitungen: <https://fsfw-dresden.de/gpg>
- ▶ temporäre E-Mailadressen zum Test:
 - ▶ Adresse/User: `pgp-test-0x@hejn.de` ($x = 1..5$)
 - ▶ Mailserver: `vega.uberspace.de`
 - ▶ IMAP, Port: 993
 - ▶ Passwort: `fingerprint`

Schlüsselgenerierung



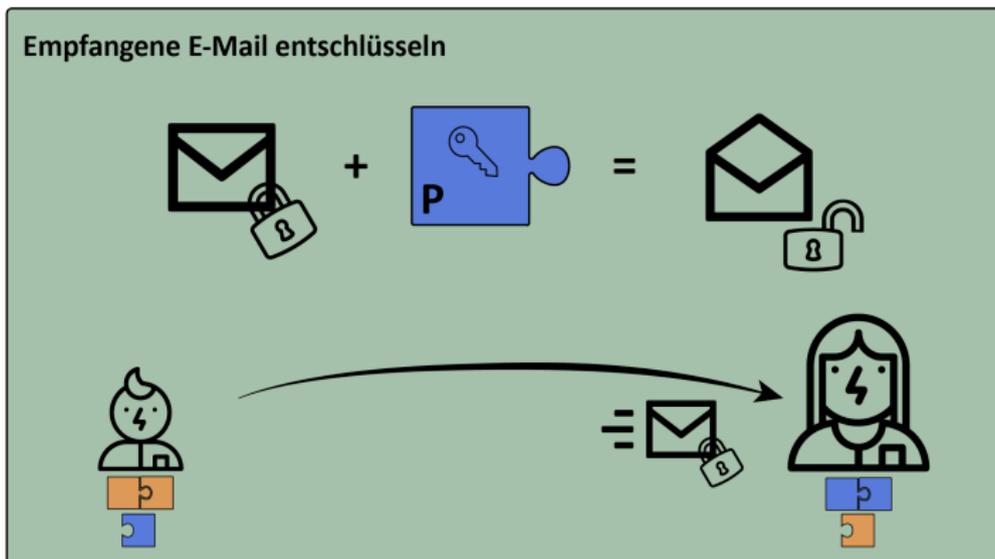
E-Mails verschlüsseln

→ ÖS müssen bereits ausgetauscht sein!



Testmail (mit Schlüssel im Anhang) an: vertraulich@hejn.de

E-Mails entschlüsseln



Ausblick – Schutzziele bei PGP

- Vertraulichkeit
- Integrität (keine Veränderung)
- Anonymität
- Verfügbarkeit

Ausblick – Schutzziele bei PGP

- Vertraulichkeit → Verschlüsselung
- Integrität (keine Veränderung)
- Anonymität
- Verfügbarkeit

Ausblick – Schutzziele bei PGP

- Vertraulichkeit → Verschlüsselung
- Integrität (keine Veränderung) → Signatur notwendig
- Anonymität
- Verfügbarkeit

Ausblick – Schutzziele bei PGP

- Vertraulichkeit → Verschlüsselung
- Integrität (keine Veränderung) → Signatur notwendig
- Anonymität
- Verfügbarkeit

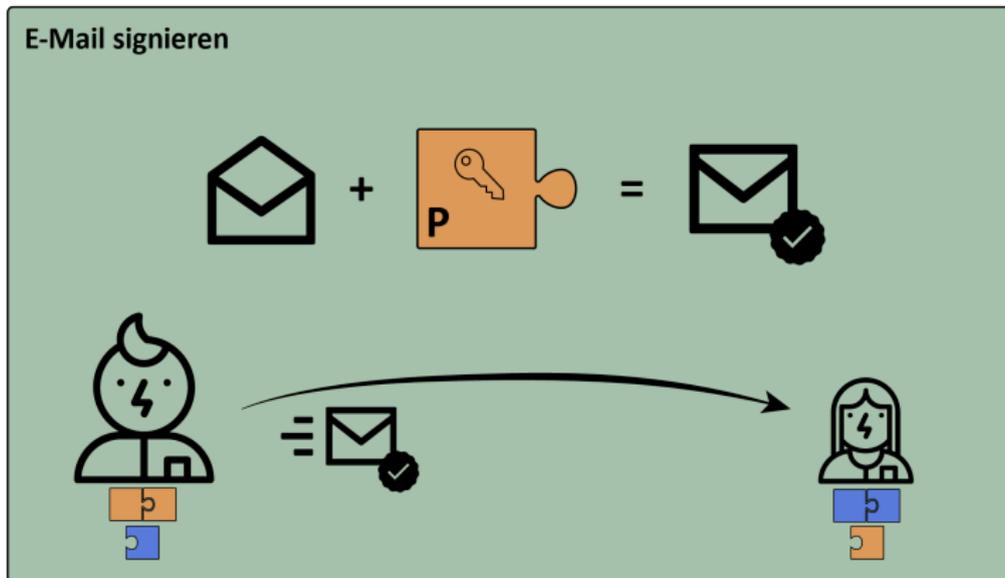
Ausblick – Signieren 1

- ▶ Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- ▶ Überprüfen = Entschlüsseln mit ÖS
- ⇒ Man muss dem öffentlichen Schlüssel vertrauen
- Integrität (keine Veränderung)

Ausblick – Signieren 1

- ▶ Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- ▶ Überprüfen = Entschlüsseln mit ÖS
- ⇒ Man muss dem öffentlichen Schlüssel vertrauen
- ☑ Integrität (keine Veränderung)
 - ▶ Schlüssel signieren bei persönlichem Treffen (Keysharing-Party) → „Web of trust“
 - ▶ Fingerabdruck-Bsp:
214E 4E9D B193 6AF2 CFDC 68DF 13AD 3604 9D3E F6BF

Ausblick – Signieren 2



Ausblick – Schlüssel pflegen

- ▶ Ablaufdatum \Rightarrow Verlängerung notwendig!
 - ggf. neu auf Schlüsselserver hochladen!

Ausblick – Schlüssel pflegen

- ▶ Ablaufdatum \Rightarrow Verlängerung notwendig!
 - \rightarrow ggf. neu auf Schlüsselsever hochladen!

- ▶ Widerrufszertifikat sichern
 - \rightarrow wir benötigt falls:
 - ▶ Passphrase vergessen
 - ▶ PS verloren (\rightarrow Backup!)
 - ▶ Vertrauen in PS verloren

Ausblick – Nachteile PGP

Was wird verschlüsselt?

- ▶ Text
- ▶ Anhänge Format-Empfehlung: PGP/MIME nicht: Inline PGP

Was wird nicht verschlüsselt?

- ▶ Metadaten
 - ▶ Absender*in, Empfänger*in, **Betreff**, ...

Weiterführendes (1)

- ▶ Datenspuren (21. - 22. Okt.)

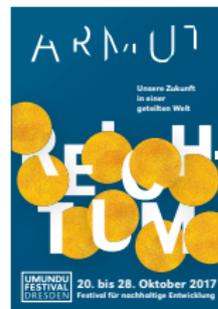
<https://www.datenspuren.de>

- ▶ Öffentliches Symposium des <http://c3d2.de/>
- ▶ Vorträge, Info-Stände, Workshops u.v.m.



- ▶ Umundu-Festival (20. - 28. Okt.)

- ▶ Festival für nachhaltige Entwicklung
- ▶ Fokus Thema 2017: Armut und Reichtum
- ▶ Filme, Vorträge, Workshops, ...
- ▶ <https://umundu.de/>



Weiterführendes (2)

PGP-Verschlüsselung für Webmail

- ▶ <https://vimeo.com/178702500> (Screencast)
- ▶ Anleitung von Posteo

Allgemeine Infos

- ▶ <https://virtual-privacy.org>

Cryptopartys

- ▶ <https://www.cryptoparty.in>
- ▶ <https://de.wikipedia.org/wiki/CryptoParty>

Radio

- ▶ Deutschlandfunk-Essay: *Niemand hat nichts zu verbergen*

Videos

- ▶ G. Greenwald: *Why privacy matters*
- ▶ J. Oliver + E. Snwoden (lustig)