+

Sichere Kommunikation: Warum & Wie

KRETA – Oktober 2017

FSFW: Wer sind wir?

- 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: Wer sind wir?

- 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 horrende Summen von Zeitschriften-Verlagen gekauft werden müssen

FSFW: Wer sind wir?

- 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 horrende 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: Wer sind wir?

- 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 horrende 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: Wer sind wir?

- 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 horrende 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: Wer sind wir?

- 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 horrende 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

- 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 und signieren
- 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
  - Erstarken totalitärer Strukturen

„Ich habe doch nichts zu verbergen“

- In Menschheitsgeschichte:
  viele Beispiele für **rücksichtslosen Egoismus**
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

„Ich habe doch nichts zu verbergen“

- In Menschheitsgeschichte:
  viele Beispiele für **rücksichtslosen Egoismus**
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

- **Digitalisierung verstärkt das Problem**
- E-Mail[1] ist wie Postkarte: unterwegs[2] lesbar
- E-Mail ist noch schlimmer als Postkarte:
  - automatisiert auswertbar
  - unbemerkt kopierbar
  - unbemerkt veränderbar (inkl. Metadaten, bspw. Absender)

1: E-Mail = nur Beispielmedium 2: ggf. um die ganze Welt

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen
- **Integrität**
  $\rightarrow$ B weiß, die Nachricht ist nur von A geschrieben, nicht verändert

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen
- **Integrität**
  $\rightarrow$ B weiß, die Nachricht ist nur von A geschrieben, nicht verändert
- **Anonymität**
  $\rightarrow$ A bestimmt, wem sie ihre Identität preisgibt

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen
- **Integrität**
  $\rightarrow$ B weiß, die Nachricht ist nur von A geschrieben, nicht verändert
- **Anonymität**
  $\rightarrow$ A bestimmt, wem sie ihre Identität preisgibt
- **Verfügbarkeit**
  $\rightarrow$ 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
- Schlüsselserver (*keyserver*)
- Fingerabdruck
- Metadaten
- Widerrufszertifikat

PGP – Das Problem

- P1) A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

PGP – Das Problem

- P1) A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

- P2) Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren

  - Es gibt: **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel

PGP – Das Problem

- P1) A möchte Nachricht an B vertraulich schicken

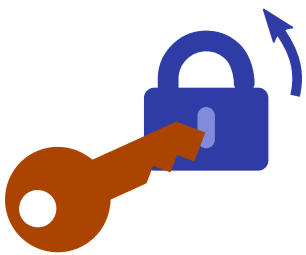
$\Rightarrow$ Nachricht verschlüsseln

- P2) Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren
  - Es gibt: **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel

- **ÖS**: zum Verschlüsseln

- **PS**: zum Entschlüsseln



PGP – Das Problem

- P1) A möchte Nachricht an B vertraulich schicken

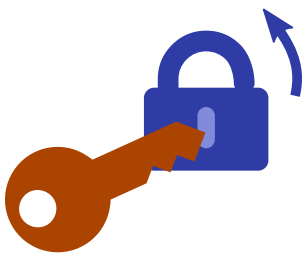
$\Rightarrow$ Nachricht verschlüsseln

- P2) Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren
  - Es gibt: **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel

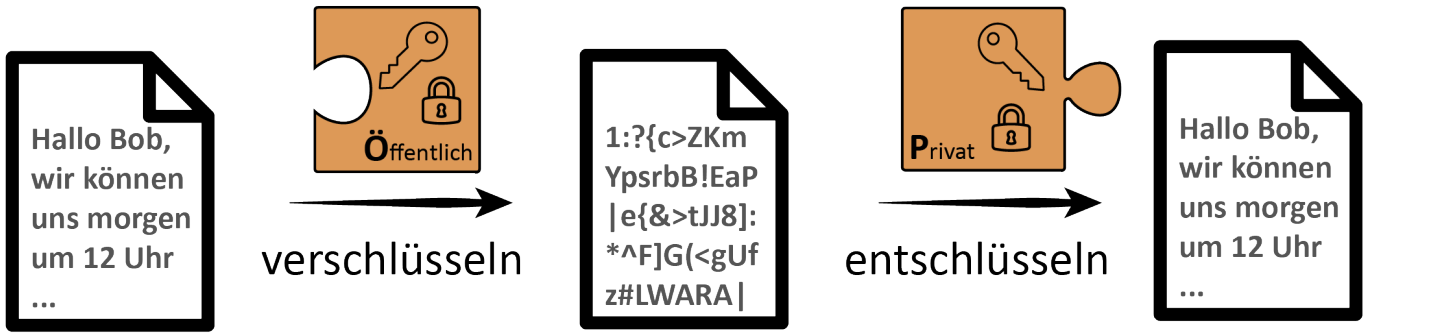
- **ÖS**: zum Verschlüsseln

- **PS**: zum Entschlüsseln



Oft eingesetzt: `GPG` (**G**nu**P**rivacy**G**uard) = freie Software

PGP – Funktionsweise 1



Daten
(Nachricht im Klartext)

verschlüsselte Daten

ursprüngliche Daten

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` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?

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` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?
- 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

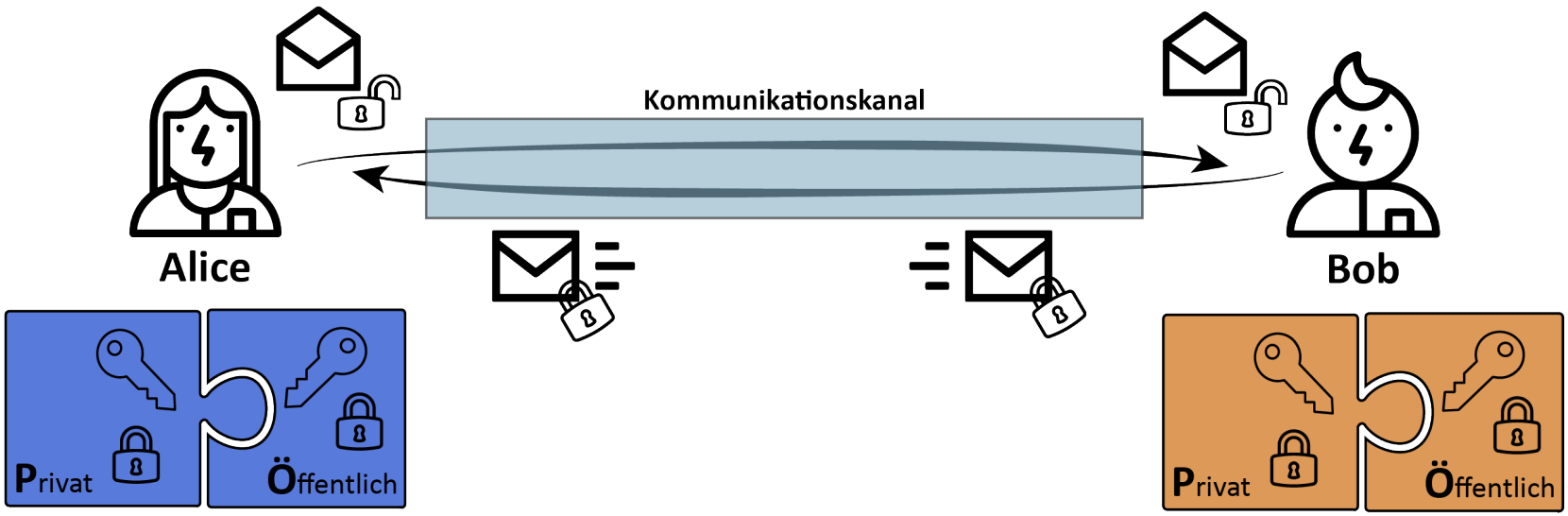
PGP – Funktionsweise 2

- 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` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?
- 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

Anleitungen

- Linux & Windows
  https://fsfw-dresden.de/gpg
- OS X
  https://gpgtools.tenderapp.com/kb/how-to/erste-schritte-gpgtools-einrichten-einen-schlssel-erst

Integrität durch Signieren

- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

$\Rightarrow$ Man muss dem öffentlichen Schlüssel vertrauen

Integrität durch Signieren

- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

$\Rightarrow$ Man muss dem öffentlichen Schlüssel vertrauen

- Schlüssel signieren bei persönlichem Treffen (Keysharing-Party) $\rightarrow$ „Web of trust“
- Fingerabdruck-Bsp: `214E 4E9D B193 6AF2 CFDC 68DF 13AD 3604 9D3E F6BF`

Ausblick

Was wird verschlüsselt?

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

Was wird nicht Verschlüsselt?

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

Weiterführendes

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)