# Emails und GPG

Von Emails und Postkarten
oder wieso
Emails verschlüsselt werden sollten



# GPG ?

GPG ist GnuPG ist Gnu Privacy Guard

Freie Variante von PGP (Pretty Good Privacy)

Eine der am meisten verwendeten Methoden um Emails zu verschlüsseln, zu signieren und sicher zu übertragen

- Kann auch Dateien usw. verschlüsseln

PGP sollte nicht verwendet werden, da es kein freies Programm ist -> keine Überprüfungsmöglichkeit der eigentlichen Funktionalität

# Weitere Begriffe

Email-Server: elektronische Poststelle

Verschlüsseln: Einen Text für Unbefugte garantiert unleserlich zu machen

Entschlüsseln: Einen verschlüsselten Text wieder lesbar machen

Signieren: Eine digitale Signatur, welche die Authentizität der Senderin bestätigt und überprüfbar macht.

# Weshalb Emails verschlüsseln?

- Sehr viele (persönliche) Informationen werden per Email verschickt
- Emails werden durch das Internet verschickt
- Internet als unsicheres Medium, in dem grundsätzlich alle Alles lesen können
- Emails wandern nach Verschicken durch das Internet und kommen an verschiedenen euch unbekannten (Email-)Servern vorbei.

# Weshalb Emails verschlüsseln? II

~~Ich habe ja nichts zu verbergen...~~

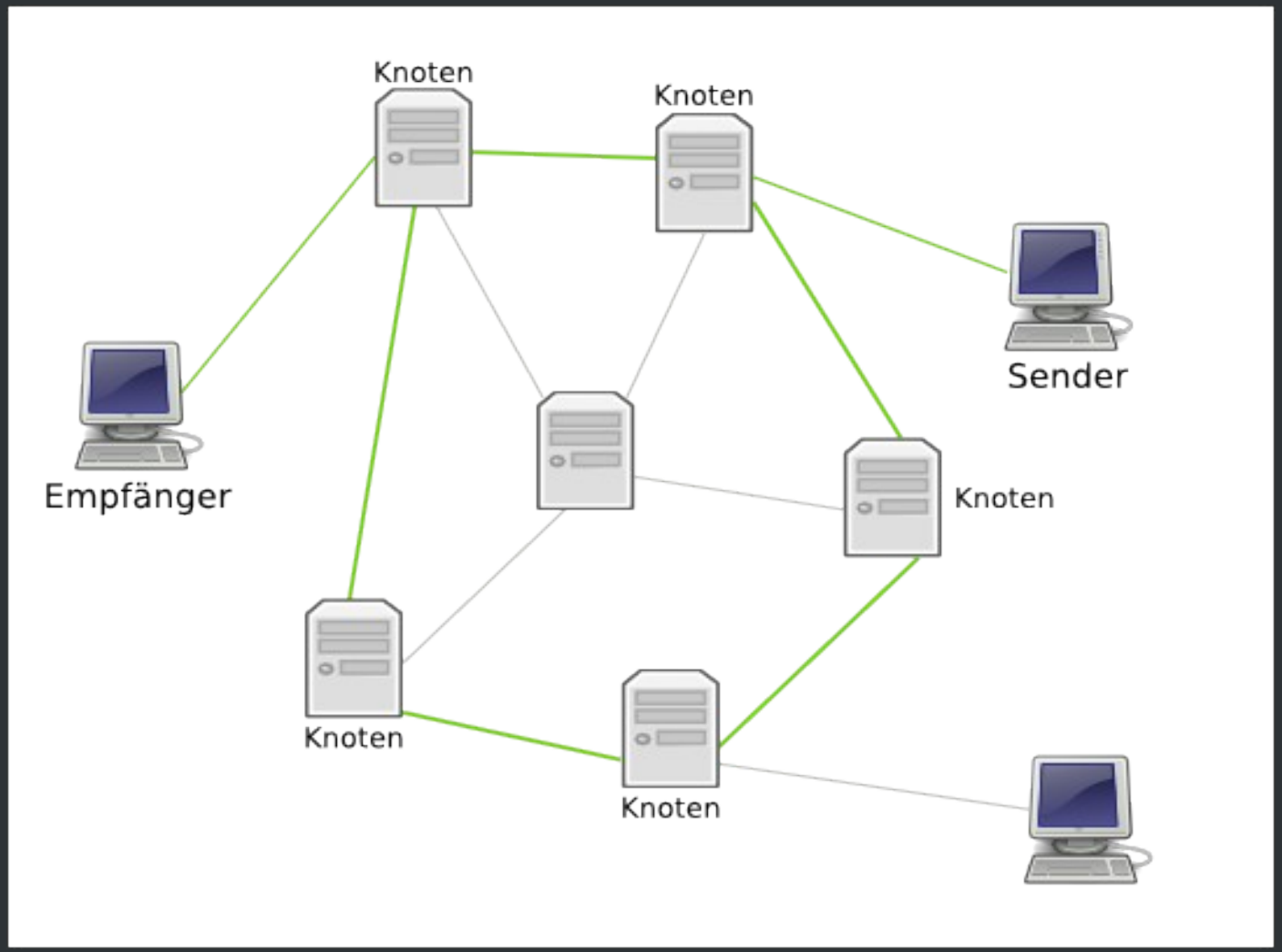
Privatsphäre!

Spam, Identitätsdiebstahl, private Schnüffelei

Staatliche Schnüffelei, Vorratsdatenspeicherung, Anti-Terror Wahn

Authentizität: Absenderadressen leicht fälschbar, mit wem maile ich genau?

# Internet – globales Netz



# Der Weg durchs Internet

Von der Senderin zur Empfängerin kommt eine Email an verschiedenen (euch unbekannten) Stationen vorbei.

Eine Email ist nichts anderes, als eine Postkarte: wer sie unterwegs lesen will, hat jederzeit die Möglichkeit dazu

**Fazit: Alles was wir per Emails verschicken, verschicken wir wie auf einer Postkarte über die normale Post.**

# Verschlüsselung

Zwei Arten von Verschlüsselung: symmetrische und asymmetrische

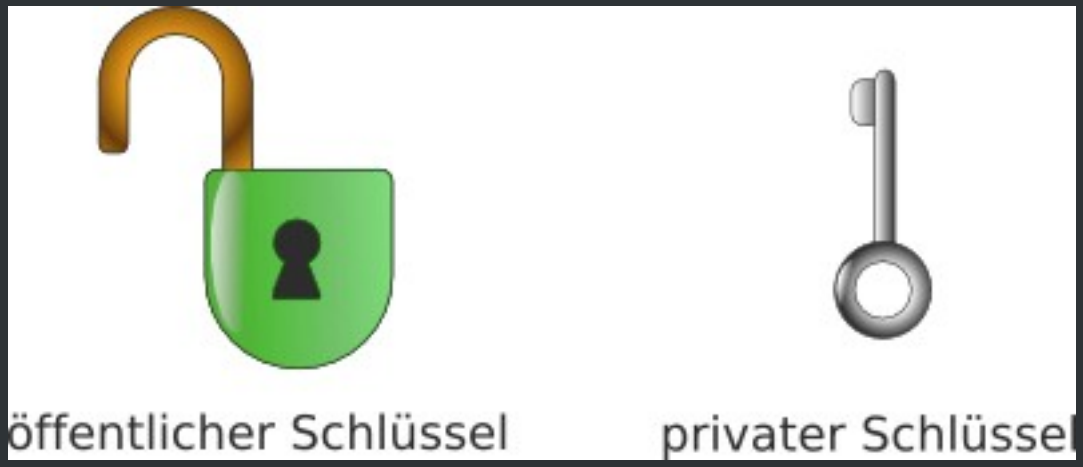
Symmetrische: Zwei Personen teilen sich einen gemeinsamen Schlüssel, mit dem sie ihre Daten sichern.

Problem: Wie tauschen wir den Schlüssel sicher aus?

**Lösung: asymmetrische Verschlüsselung**

# asymmetrische Verschlüsselung

Jede Person besitzt ein Schlüsselpaar:




Für die Ver- oder Entschlüsselung wird jeweils einer der beiden benötigt.

Die Umkehrung ist nur mit dem jeweils anderen möglich.

# asymmetrische Verschlüsselung II

Verteilung meines öffentlichen Schlüssels an alle die **mir** eine verschlüsselte Nachricht senden möchten.

Öffentlicher Schlüssel als offenes Schloss, zu dem nur ich den passenden Schlüssel (mein privater Schlüssel) zum öffnen besitze.

Basiert auf mathematischen Grundlagen.

# Verschlüsselung

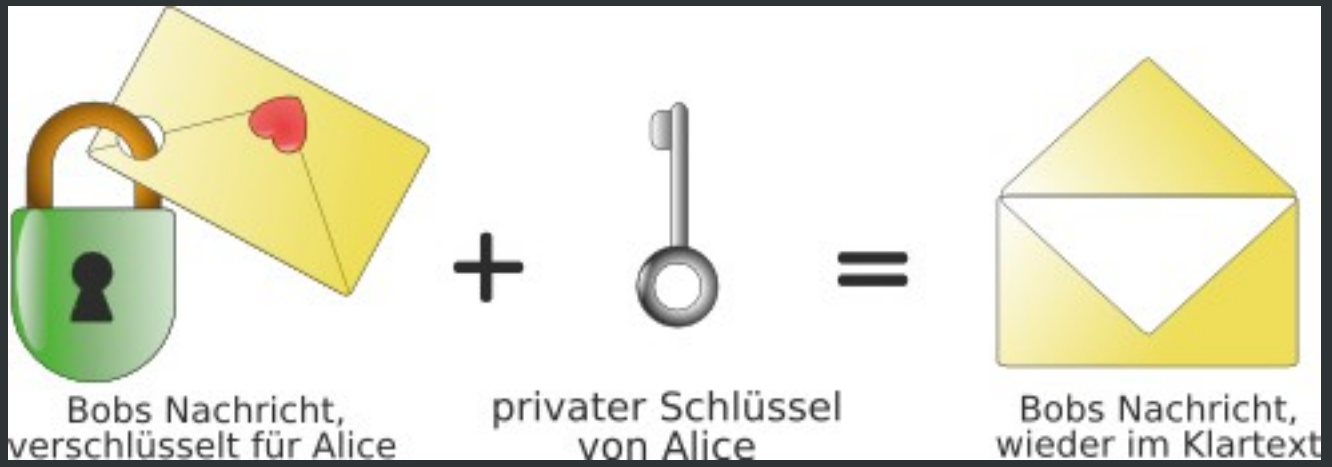
Bob möchte eine sichere Nachricht an Alice schicken

Verschlüsselung mit Alice's öffentlichen Schlüssel


Übermittlung -> niemand kann es mehr lesen

# Entschlüsselung

Alice möchte Nachricht von Bob, welche mit ihrem öffentlichen Schlüssel verschlüsselt wurde, entschlüsseln:




Die Email von Bob kann nur Alice lesen, da nur sie den passenden Schlüssel dazu hat

# Authentizität / Signieren

Fälschung von Absenderadressen ohne weiteres möglich
-> digitale Bestätigung des Senders? -> digitale Signatur

öffentlicher Schlüssel von Bob ist allen (auch Alice) bekannt

Bob fügt eine Signatur hinzu, die durch seinen eigenen privaten Schlüssel entstanden ist

Kann zusätzlich zur Verschlüsselung oder alleinstehend, falls z.B. das gegenüber (noch) keinen Public-Key besitzt, angewendet werden

# Authentizität / Signieren II

Nur Bob kann die Nachricht mit **seinem** privaten Schlüssel unterschreiben, jedoch:

Alle können mit Hilfe des öffentlichen Schlüssels von Bob überprüfen, dass die Signatur, die durch den privaten Schlüssel von Bob zustande kam, gültig ist, da nur diese beiden zusammen passen

-> Bob, und wirklich nur Bob, hat die Nachricht unterschrieben, also muss sie auch von ihm stammen

# Schlüsselverteilung

Wie mache ich meinen Schlüssel möglichst allen Leuten bekannt?

nicht so toll und bequem: alle fragen mich nach meinem öffentlichen Schlüssel

einfacher und bequemer:

- Publizierung des öffentlichen Schlüssel auf einer Homepage
- Publizierung des öffentlichen Schlüssels auf einem Schlüsselserver -> **Abfrage von noch unbekannten Schlüsseln ist in GPG-Tools bereits integriert**

# Schlüsselverteilung II

Schlüssel von Alice wird auf einem Keyserver gefunden...

... aber wie kann Bob sichergehen, dass der angebliche Public-Key von Alice auch wirklich von ihr ist?

Zwei Möglichkeiten:

- Überprüfung und Validierung des Public-Keys
- Web-Of-Trust

# Überprüfung durch Fingerprint

Jeder Key besitzt einen Fingerprint:

kurze eindeutige Zeichenfolge, z.B.
4CE0 9C3F 87E1 307B 7F36  EE12 8154 2359 1B71 49FC

ermöglicht Identifikation des Keys

Alice teilt Bob über einen sicheren Kanal (zum Beispiel bei einem persönliches Treffen) den Fingerprints ihres Key mit

Bob vergleicht diesen Fingerprint mit dem Fingerprint des heruntergeladenen Keys

Bei Übereinstimmung ist Bob in Besitz des richtigen Schlüssels

# Web-Of-Trust

Bob kann den Public-Key von Alice signieren und bürgt damit für die Validität des Keys von Alice

Olga will Alice ein Email schreiben, hat jedoch keine persönliche Kontaktmöglichkeit mit ihr

Olga vertraut jedoch Bob voll und ganz und da Bob für den öffentlichen Schlüssel von Alice bürgt und dieser von ihm signiert wurde, darf nun Olga auch dem öffentlichen Schlüssel von Alice vertrauen
-> Vertrauen über mehrere Leute hinweg möglich

# Benötigte Programme

Lokales Emailprogramm:

- Emailprogramm: Thunderbird als freie Software
- GnuPG: führt die Ver- und Entschlüsselungen durch, verwaltet den Schlüsselbund, etc.
- Enigmail: Schnittstelle zwischen GnuPG und Thunderbird

Webmail-Clients, welche die GPG-Funktionalität beinhaltet. Z.B. bei riseup.net oder immerda.ch

- bedeutend **weniger sicher** als lokales Emailprogramm, da zusätzliches Vertrauen in die Betreiberinnen bestehen muss, da diese über die privaten Schlüssel verfügen können

# Zum Ausprobieren:

CryptoCD

- Live-CD für Mac OS X, Windows und GNU/Linux mit den entsprechenden Programmen -> Ausprobieren ohne Installation und Konfiguration
- weiterführende Erklärungen zu Verschlüsselung und Installationshilfen auch von weiteren Kommunikations-programmen wie Jabber
- cooles Projekt / coole Leute (Danke für die Grafiken!)

Homepage: http://cryptocd.org
Online Version: http://cryptocd.org/online_version/

# Mehr Infos

Wiki von immerda.ch

Wikipedia: http://de.wikipedia.org/wiki/GnuPG

Who can you trust? Weitere Überlegungen von so36.net: https://www.so36.net/Home/22.html

Online Version der Crypto-CD: http://cryptocd.org/online_version/

Internet ... ;-)