Von Emails und Postkarten oder wieso Emails verschlüsselt werden sollten

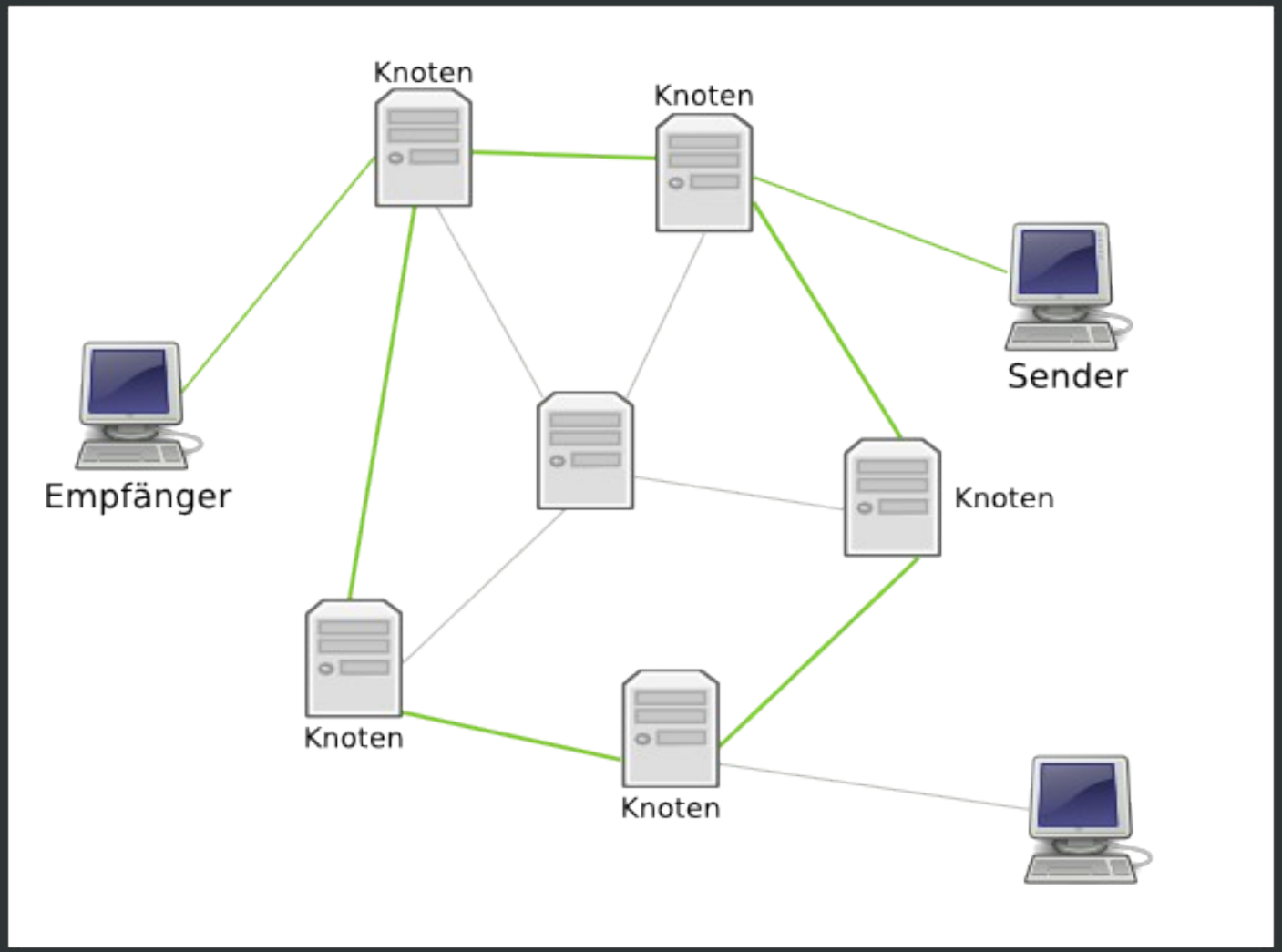
immerda project group - http://www.immerda.ch / admin(ät)immerda.ch – Version 1.0

- GPG ist GnuPG ist Gnu Privacy Guard
- Freie Variante von PGP (Pretty Good Privacy)
- Eine der am meisten verwendete Methoden um Emails zu verschlüsseln, zu signieren und sicher zu übertragen

- 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.

- 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 Emailservern vorbei.

- ~~Ich habe ja nichts zu verbergen...~~
- Privatsphäre!
- Spam, Idenditätsdiebstahl, private Schnüffelei
- Staatliche Schnüffelei, Vorratsdatenspeicherung, Anti-Terror Wahn
- Authentizität: Absenderadressen leicht fälschbar, mit wem maile ich genau?


Knoten
Knoten
Sender
Empfänger
Knoten
Knoten
Knoten

- Von der Senderin zur Empfängerin kommt ein Email an verschiedenen (euch unbekannten) Stationen vorbei.
- Ein Email ist nichts anderes, als eine Postkarte: wer es 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.**

- Zwei Arten von Verschlüsselung: symetrische und asymetrische
- Symetrische: Zwei Personen teilen sich einen gemeinsamen Schlüssel, mit dem sie ihre Daten sichern.
- Problem: Wie tauschen wir den Schlüssel sicher aus?
- **Lösung: asymetrische Verschlüsselung**

- Jede Person besitzt ein Schlüsselpaar:

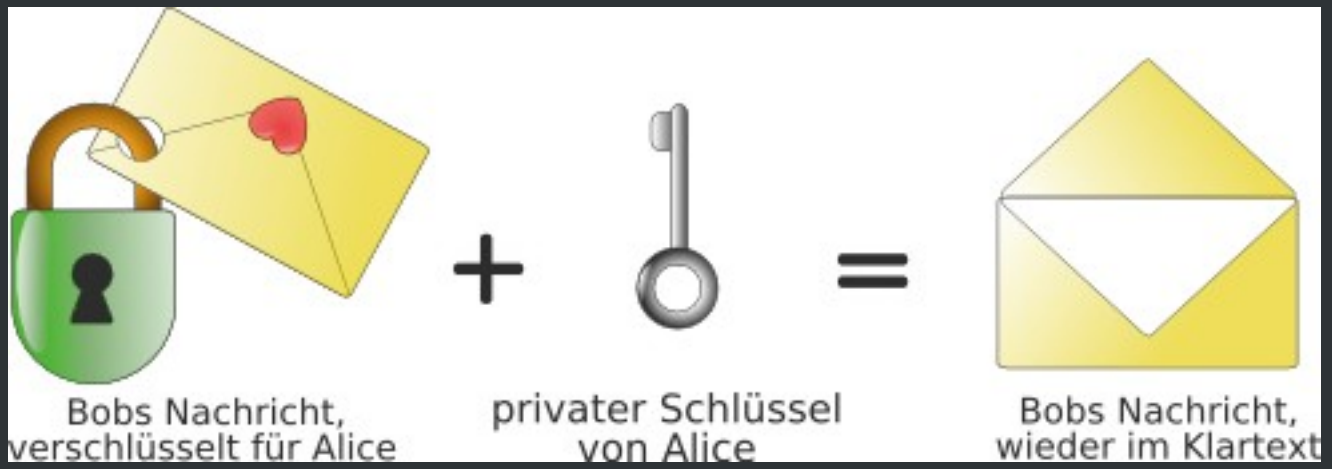
- Für die Ver- oder Entschlüsselung wird jeweils einer der beiden benötigt.
- Die Umkehrung ist nur mit dem jeweils anderen möglich.

- 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.

- Bob möchte eine sichere Nachricht an Alice schicken
- Verschlüsselung mit Alice's öffentlichen Schlüssel

- Übermittlung -> niemand kann es mehr lesen

- 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

- Fälschung von Absenderadressen ohne weiteres möglich -> digitale Bestätigung des Senders? -> digitale Signatur
- öffentlicher Schlüssel von Bob ist allen (auch Alice) bekannt
- Zusätzlich zur Verschlüsselung mit Public-Key von Alice fügt Bob eine Signatur hinzu, die durch seinen eigenen privaten Schlüssel entstanden ist

- 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

- 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
  - weniger sicher als lokales Emailprogramm, da zusätzliches Vertrauen in die Betreiberinnen bestehen muss

- CryptoCD
  - Live-CD für Mac OS X, Windows und 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/