

# Cryptoparty

## Sichere Kommunikation im Internet

Stratum 0 e. V.

17. August 2013

# Begrüßung

- Wer sind wir?
- Wer seid ihr?

# Organisatorisches

- Ablauf:
  - kurzer Vortrag zur Theorie (15-20 Min)
  - Workshop in Kleingruppen
- Getränke hinten an der Theke
- WLAN-Passwort ist: FIXME
- Folien gibts auf <https://stratum0.org/cryptoparty>

# Motivation

- Daten im Internet sind vergleichbar mit Postkarten:



# Motivation

- Daten im Internet sind vergleichbar mit Postkarten:



- Mögliche Angriffspunkte:
  - Provider A
  - die große Internet-Wolke
  - Provider B

# Motivation

- Daten im Internet sind vergleichbar mit Postkarten:



- Mögliche Angriffspunkte:
  - Provider A
  - die große Internet-Wolke
  - Provider B
- Aber: es gibt Möglichkeiten, das zu verhindern.

## Disclaimer

- Es gibt keine 100-prozentige Sicherheit.
- Alles hier gezeigte ist Stand der Technik und hinreichend sicher.

Trotzdem: plant keine Terroranschläge über das Internet.

# Public-Key-Kryptografie

*(Kryptografie: die Lehre vom Geheimen)*

- 1977 erfunden von Ron Rivest, Adi Shamir und Leonard Adleman
- komplizierte mathematische Verfahren
  - soll hier nicht erklärt werden
- Jeder Kommunikationsteilnehmer generiert ein zufälliges Schlüsselpaar:
  - einen öffentlichen Schlüssel zum Verschlüsseln von Nachrichten
  - einen geheimen Schlüssel zum Entschlüsseln von Nachrichten

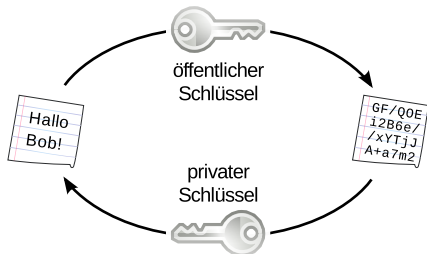
## Achtung

Der private Schlüssel sollte geheim gehalten werden, der öffentliche Schlüssel sollte veröffentlicht werden.






# Public-Key-Kryptografie

- Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem passenden privaten Schlüssel entschlüsselt werden



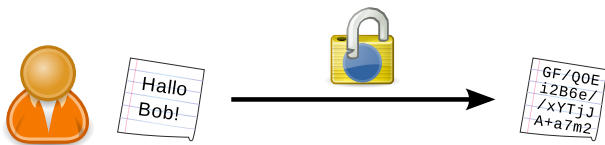
- der private Schlüssel kann nicht aus dem öffentlichen Schlüssel hergeleitet werden

# Analogie

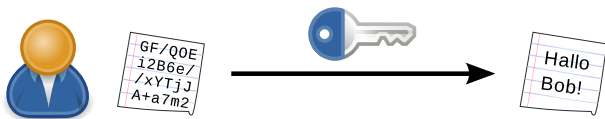
- Das ist Bob: 
- Bob verteilt Bügelschlösser für jeden, der Nachrichten an ihn verschlüsseln will: 
  - öffentlicher Schlüssel
- Bob behält den Schlüssel für die Schlösser: 
  - privater Schlüssel

# Verschlüsseln und Entschlüsseln

Alice verschlüsselt eine Nachricht an Bob mit seinem öffentlichen Schlüssel:

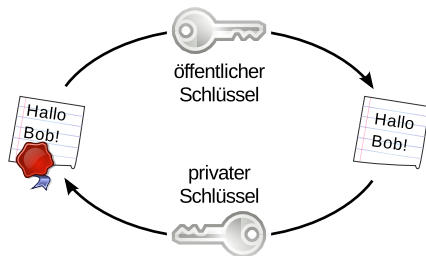


Nur Bob kann diese Nachricht jetzt mit seinem privaten Schlüssel lesen:



# Signaturen

Das System auch umgekehrt für Signaturen einsetzbar:



- Bob verschlüsselt ein Dokument mit seinem *privaten* Schlüssel
  - nur Bob hat diesen privaten Schlüssel, also kann nur Bob diesen Schlüsseltext erstellt haben
- Jeder andere kann den Schlüsseltext entschlüsseln und Bobs Signatur überprüfen

# Vertrauensnetzwerke

Soweit in Ordnung...

Aber wie kann ich sicher sein, dass der Schlüssel, mit dem ich Nachrichten verschlüssele, auch wirklich Bob gehört?

# Vertrauensnetzwerke

Soweit in Ordnung...

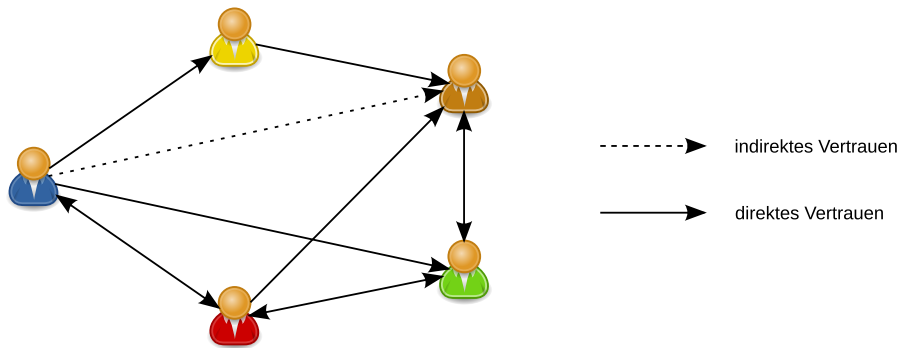
Aber wie kann ich sicher sein, dass der Schlüssel, mit dem ich Nachrichten verschlüssele, auch wirklich Bob gehört?

**Lösung:** Vertrauensnetzwerke

- Ich prüfe, ob Alices öffentlicher Schlüssel auch wirklich Alice gehört
  - Falls ja, signiere ich ihren öffentlichen Schlüssel
  - Ich versichere damit, dass Alice diesen Schlüssel besitzt
- Alice hat das gleiche mit Bobs Schlüssel getan
- Falls Alice nicht schlampig war, kann ich Bobs Schlüssel indirekt vertrauen

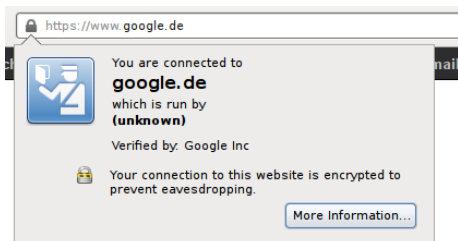
# Vertrauensnetzwerke

Beispiel Vertrauensnetzwerk:



# Sicher surfen: HTTPS

- Webserver besitzt privaten und öffentlichen Schlüssel („Zertifikat“)
- Schlüsselerzeugung auf Benutzerseite dynamisch
- Vertrauensnetzwerk über *Certificate Authorities* (CA)
  - nehmen meist Geld für die Signatur des Server-Zertifikats
  - Identitätsprüfung je nach CA unterschiedlich genau...
  - Browser vertrauen nur bestimmten CAs ⇒ Zertifikatswarnungen





# Sicher surfen: HTTPS

## Achtung

Die Daten sind nur auf dem Weg zum Webserver geschützt, am Ende liegen sie wieder entschlüsselt vor!

- Auf dem Webserver könnte z. B. auch ein Angreifer seine Finger im Spiel haben...
- Certificate Authorities könnten gefälschte Zertifikate ausstellen
  - Beispiel: Comodo CA, DigiNotar, TürkTrust
- keine eingebaute Anonymisierung

# Mails verschlüsseln: PGP

- PGP: Pretty Good Privacy („Ziemlich gute Privatsphäre“)
- seit 1998 ein Standard für Mailverschlüsselung
  - Freie Softwarelösung: GnuPG (GNU Privacy Guard)
- Verschlüsselt keine Metadaten (wie z. B. Betreffzeile)!
- Erweiterungen für viele Mailprogramme vorhanden

## Webbasierte Dienste?

Mit webbasierte Diensten ist PGP kaum möglich – es ist nötig, ein Mailprogramm auf dem eigenen Rechner zu installieren! Die meisten Anbieter bieten Anleitungen zum Einrichten der Mailkonten im Mailprogramm an.

# PGP: Softwareunterstützung

- Windows: Gpg4Win, <http://gpg4win.org/>
- Mac OS X: GPGTools, <https://www.gpgtools.org/>
- Linux: GnuPG, <http://gnupg.org>

Darauf aufbauend Unterstützung in Mailprogrammen:

- Mozilla Thunderbird: Enigmail, <http://enigmail.org>
- Apple Mail: GPGMail, <https://www.gpgtools.org/>
- Microsoft Outlook: Gpg4Win

# Chats verschlüsseln: OTR

- OTR: Off-the-Record Messaging
- Verschlüsselung
- Authentizität
- Abstreitbarkeit
  - keiner kann nachher beweisen, ich hätte etwas bestimmtes gesendet
- Folgenlosigkeit
  - Verlust des privaten Schlüssels hat keine Auswirkung auf bisherige Verbindungen

## OTR: Softwareunterstützung

- eingebaut in Adium (Mac OS X), Jitsi, Xabber (Android), ChatSecure (iOS)
- Pidgin (Windows, Linux): <http://www.cypherpunks.ca/otr/>
- Miranda (Windows): auf der Addons-Seite

### Tipp

Adium, Pidgin und Miranda unterstützen alle gängigen Netzwerke, z. B. ICQ, MSN, Yahoo und auch Facebook Chat.

## Weitere Informationen

- CryptoCD, Anleitungen auf deutsch,  
<http://www.cryptocd.org/CryptoCDBetriebssystem>
- Cryptoparty Handbook, mit Anleitungen zu allen hier gezeigten Themen (englisch),  
<https://www.cryptoparty.in/documentation/handbook>

# Quellen

Folgende Bilder wurden benutzt:

- Server-Icon, Computer-Icon: aus dem Tangerine-Icon-Theme, CC-BY-SA 2.5, Copyright 2004-2006 Canonical Ltd.
- Schlüssel-Icon: aus dem Gnome-Icon-Theme, CC-BY-SA 3.0 United States, Copyright GNOME Project
- Notizblock-Icon: [http://commons.wikimedia.org/wiki/File:Ruled\\_paper\\_note\\_with\\_pin.svg](http://commons.wikimedia.org/wiki/File:Ruled_paper_note_with_pin.svg), Autor: Andreas Plank, CC-BY-SA-3.0 Unported
- alle anderen Icons aus dem Tango Project, gemeinfrei.