# MAILS VERSCHLÜSSELN

## MIT PGP

**„Encryption works.
Properly implemented strong crypto systems are
one of the few things that you can rely on.“**

***Edward J. Snowden, 17. Juni 2013***

PIRATEN PARTEI



Selbstbestimmt.Digital e.V.
gemeinsam Zukunftsräume gestalten
www.selbstbestimmt-digital.de

# WAS BISHER GESCHAH:

- **Zahlreiche Enthüllungen zur NSA durch Edward Snowden**, mit Hilfe von Laura Poitras und Glenn Greenwald seit Juni 2013
- **Größter Überwachungsskandal der Geschichte**: Geheimdienste NSA, GCHQ und BND hören den **gesamten Internetverkehr weltweit** ab und speichern alles für 30 Tage
- **Geheimdienste handeln ohne demokratische Kontrolle**: Untersuchungsausschuss #NSAUA bekommt weitgehend geschwärzte Akten, viele Befragungen sind **nicht öffentlich**.
- **Bundesregierung und Kanzlerin Merkel** zeigen kein Interesse an Aufklärung oder Veränderung, das Motto: **„Vertuschen, verschleiern, aussitzen."**

→ **Politische Veränderung dauert lange.**


DIE WAHRHEIT SAGEN?
PFUI DEIBEL!

# FOLGEN FÜR DEN EINZELNEN …

- **Verlust der Reisefreiheit**:
  Einreise in USA ohne Grund verweigert, **No-Fly-Liste**:
  Reiseverbot bei „Computerstraftaten“ in Frankreich geplant.
- **Finanzieller Verlust:** „Bin Laden“ im Verwendungszweck:
  Konto gesperrt, Kredite werden nicht mehr genehmigt.
- **Unbewusste Anpassung aus Angst** vor Überwachung:
  - **Meinungsfreiheit:** Selbstzensur bei digitaler Mediennutzung
  - **Versammlungsfreiheit:** Nicht mehr an Demos teilnehmen
  - **Privatsphäre:** Selbstzensur auch im Privatleben

→ **Chilling Effects in der Gesellschaft**

# … UND FÜR DIE GESELLSCHAFT

- **Überwachung ist abstrakt, nicht spürbar!**
- Gesellschaftliche **Veränderungen sind schleichend**!
- Bewusstsein für **Grundrechte und Demokratie** sinkt
- **Aber: Jeder hat etwas zu verbergen!**
- Vertrauen in **Technik**, **Gesellschaft und Wirtschaft** sinkt: Innovation, Kreativität, Wirtschaftskraft wird geschwächt
- **Unabhängigkeit von Politik und Medien:** Gefahr von Erpressbarkeit und Manipulation, Einschüchterung und Verfolgung

**→ Unsere Demokratie ist in Gefahr!**

# WAS KÖNNEN WIR TUN?

- **Politisch und gesellschaftlich aktiv werden:**
  - **Menschen** in unserem Umfeld **wachrütteln**!
  - **Wissen** und Kenntnisse zu Verschlüsselung **teilen**!
  - **Für Grundrechte** demonstrieren: **Freiheit statt Angst!**
- **Die Chancen der Digitalisierung nutzen:**
  - **Freie Software** und Anonymisierung **verwenden**!
  - **Verschlüsselt kommunizieren** – was ist noch sicher?:
    - **Messenger** mit OTR: Pidgin mit OTR-Plugin
    - **Smartphone**: TextSecure, RedPhone und Signal
    - **E-Mail:** Verschlüsselung mit PGP

**→ Wer verschlüsselt ist wieder frei! \o/**

# WAS IST VERSCHLÜSSELUNG?

- **Verschlüsselung** (Chiffrierung) wandelt mit Hilfe eines **Verschlüsselungsverfahrens** (Chiffre) lesbaren **Klartext** (Dechiffrat) in unleserlichen **Geheimtext** (Chiffrat) um.
- Beispiel
  - Klartext: `Geheimbotschaft`
  - Geheimtext:

```
hQIMA2f18waqUmWwARAAgqev8bFnetgNoVrcUxX0KWF64OAEiGm+ZOmBbHhCU0Ju
McR2H2zkHY1oEpx84qPaGV4zcKLxLpjovpeZavMUFGKedGmHphMzcAs7PsU1lqgK
GgdY7E4FZ8fMAYnTuo78jHxyJ4hi9afjg6JjYCZo11p6IR54R52/uFOCJ6wDfcfo
90Z2v6PgY6H2CclPDV4kuZlUrbIcjQfGmF5ZLbjOy4/c00p5cMUYa8o5hLvkw24s
DDBrdqCQsIYCI9gyrwUZr8xahES4fXIlPX7RwQegAD0rRzxLEJxFdSs4ZkpFwZ/r
PX3b6wO/ON1FZLb3QiPsEdhw99FxVsqxItFz4IS01obZHycsM8bEd5KGTJhBvHv5
pA/KhOGxeKqVEJ5BdOGb4q1qRrmtHpFTQlId1pt+jScr/a/Qy88NryOfBFidfTjH
RZr7K3rlq/rQSnegtpUxiDIpAxoMi5ACJJMXYiqm2u6NorVMXEyc/Af7P+1IwQPu
kdDox5Sgb8YkBs3dZKXYX9TvuoYadaAyGQ9SacNReucZqC+7s11koBaaO7Lu2EEa
J6RnloHAtMjlKWVxJ8aUOfusCKcaKZAax66TMQWgd5FhLpVYDdeUXavz3XkJBoZD
vH5wWfQJNGOgPozNYX4yX2Zd5caWdUClu85ocCTbi/kk6qGneQFMmu1KPDZYUHfS
VwGj0cHVATMaJDFKt645ZDMMOnOsORye3pvXH/RWvaZ1SfkdNWFHoXA/Z5YXrWfZ
jIaDlfFV8pwUsgkNezunEPd9sS+LUC8HjYHiKhMQyPIzNHe6ZIT+jw==
=I1PE
```

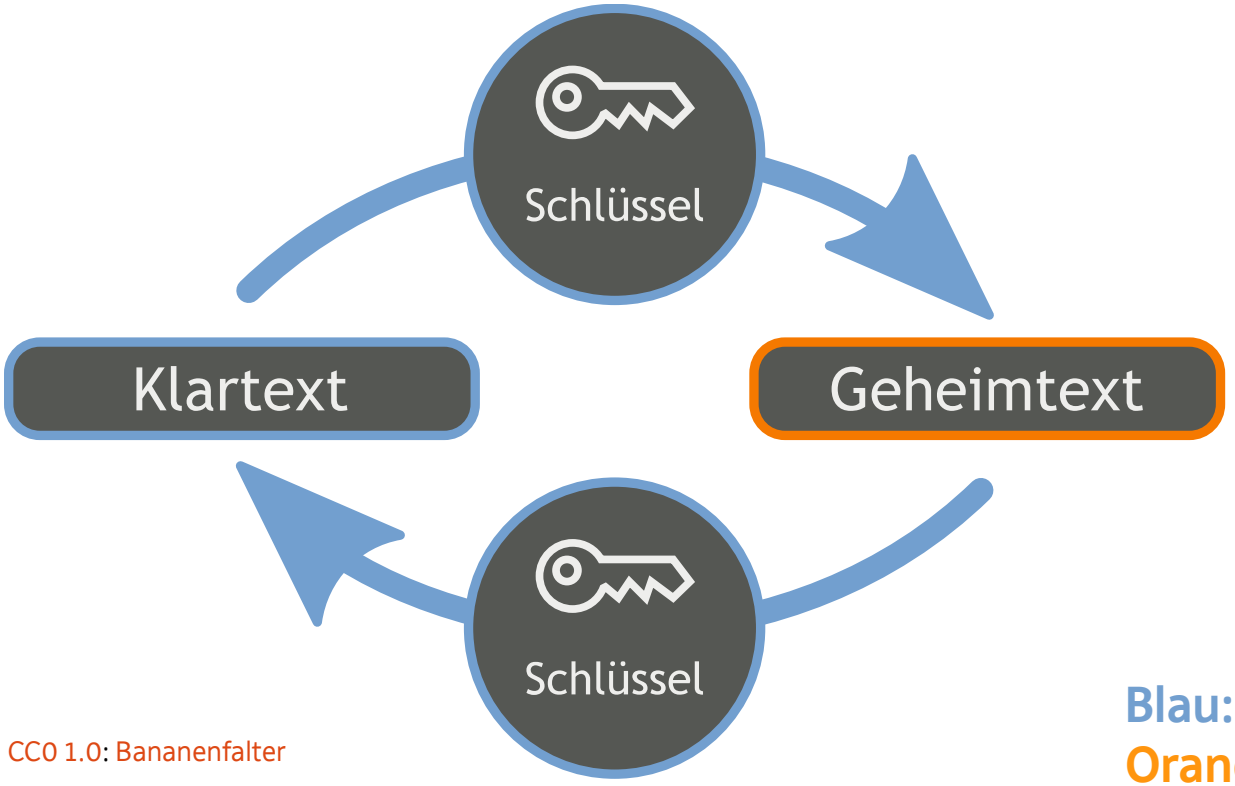
# WIESO VERSCHLÜSSELUNG?

- Verschlüsselung hat vier Hauptziele zum **Schutz von Informationen**:

  1) **Vertraulichkeit/Zugriffsschutz:** Nur berechtigte Personen dürfen die Nachricht lesen.
  2) **Integrität/Änderungsschutz:** Die Nachricht muss vollständig und unverändert sein.
  3) **Authentizität/Fälschungsschutz:** Der Urheber der Nachricht muss eindeutig identifizierbar sein.
  4) **Verbindlichkeit/Nichtabstreitbarkeit:** Der Urheber kann seine Urheberschaft der Nachricht nicht abstreiten.

# SYMMETRISCHE VERSCHLÜSSELUNG

- Nutzung **desselben** Schlüssels für Ver- und Entschlüsselung, wodurch Vertraulichkeit gewährleistet wird.

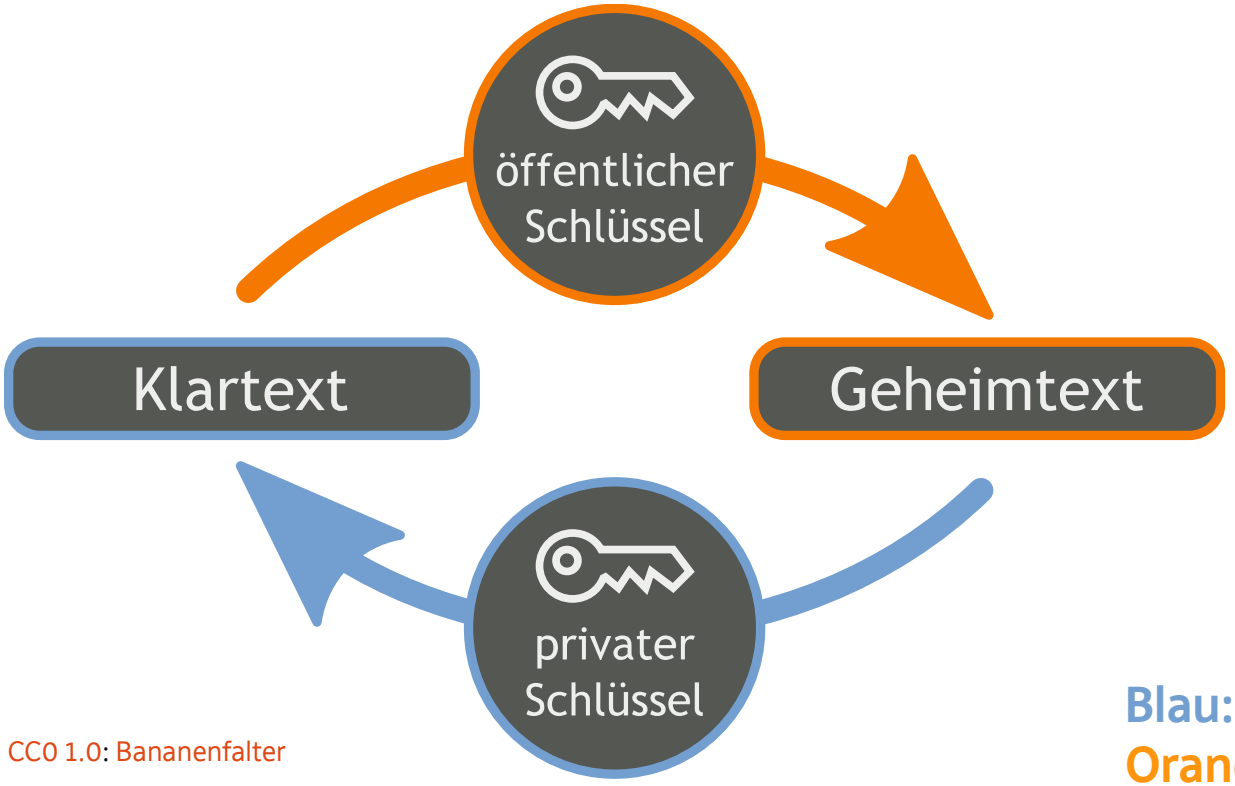





Blau: geheim
Orange: öffentlich

# ASYMMETRISCHE VERSCHLÜSSELUNG

- Nutzung eines **Schlüsselpaares** bestehend aus einem **privaten** und einem **öffentlichen** Schlüssel für die Ver- und Entschlüsselung.

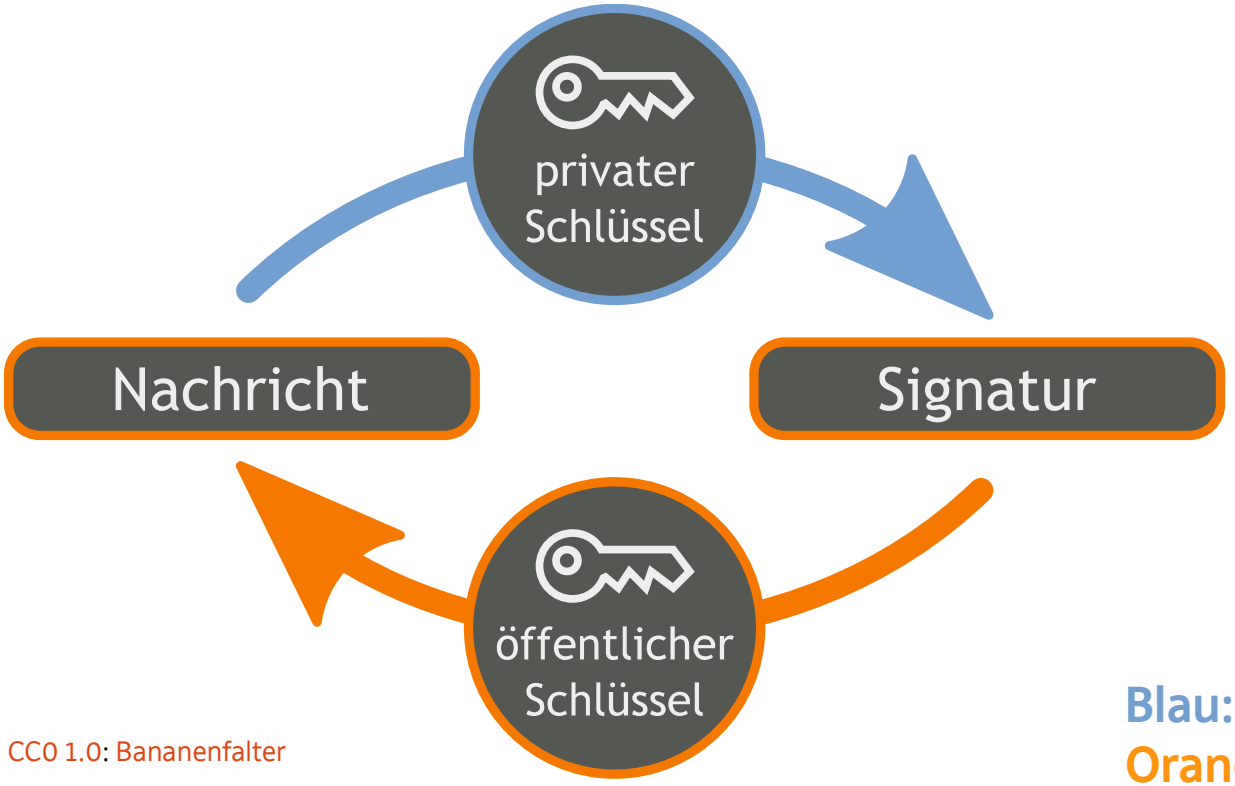





**Blau:** **geheim**
**Orange:** **öffentlich**

# ASYMMETRISCHE VERSCHLÜSSELUNG

- Mit demselben Schlüsselpaar können Nachrichten auch mit einer **Signatur** versehen bzw. unterschrieben werden, um die Integrität, Authentizität und Verbindlichkeit sicherzustellen.






**Blau: geheim**
**Orange: öffentlich**

# PGP? OPENPGP? GPG? WTF?

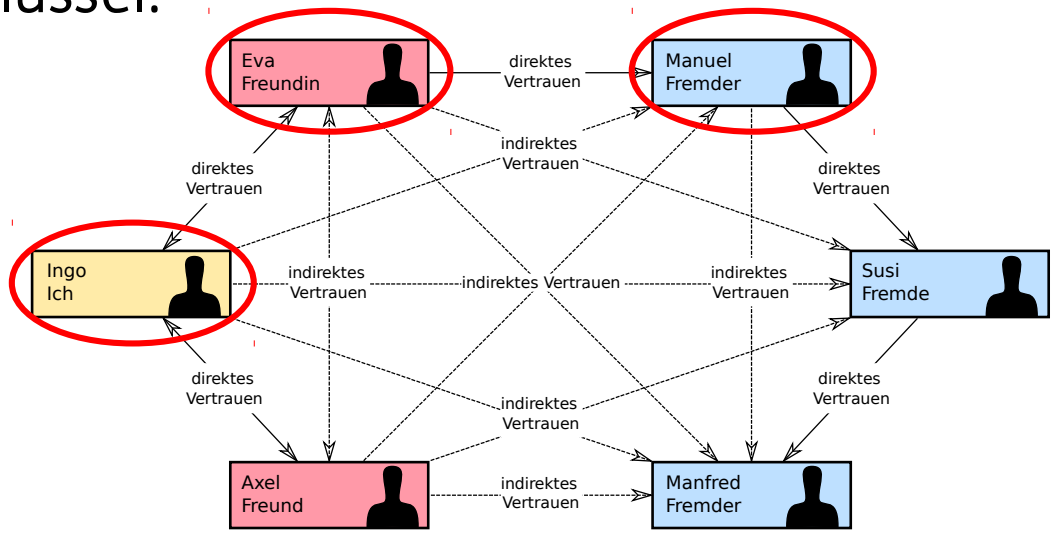
- **PGP** (Pretty Good Privacy)
  - Software zum Verschlüsseln und Signieren von Daten, die 1991 von Phil Zimmermann veröffentlicht wurde.
- **OpenPGP**
  - Offizieller Standard, der auf PGP 5 basiert.
  - PGP beinhaltete patentierte Algorithmen, war kommerziell und proprietär und durfte nicht aus den USA exportiert werden.
- **GPG/GnuPG** (GNU Privacy Guard)
  - Software zum Verschlüsseln und Signieren von Daten, die als freier Ersatz für PGP entwickelt wurde.
  - Implementiert den OpenPGP-Standard.

# WEB OF TRUST (NETZ DES VERTRAUEN)

- Schlüssel sind auf öffentlich zugänglichen **Schlüssel-Servern** abgelegt und können dort nicht mehr entfernt werden. Es besteht aber die Möglichkeit eines **Schlüsselwiderrufs**.
- **Problem:** Eine Person könnte einen Schlüssel veröffentlichen, mit welchem sie sich als jemand anderes ausgibt.
- **Lösung:** Die Echtheit öffentlicher Schlüssel wird von einer vertrauenswürdigen Instanz durch ein digitales Zertifikat bestätigt. Dies geschieht entweder durch
  - zentrale **Zertifizierungsstellen**, wie z.B. Unternehmen, öffentlichen Organisation oder auch Regierungsstellen
  - oder durch die **Teilnehmer eines Web of Trust** selbst.

# WEB OF TRUST (NETZ DES VERTRAUEN)

- Durch **Signieren** des öffentlichen Schlüssels einer anderen Person bestätigt man dessen Echtheit.
- **Direktes Vertrauen**
  - Ingo signiert Evas Schlüssel.
  - Eva signiert Manuels Schlüssel.
- **Indirektes Vertrauen**
  - Somit vertraut Ingo auf indirektem Wege ebenfalls Manuel.



# WEB OF TRUST (NETZ DES VERTRAUEN)

- Durch Schlüssel-Server entstehen auch Problematiken:
  - **Preisgabe personenbezogener Daten**:
    - Wer hat meinen Schlüssel signiert?
    - Wer gehört zu meinem sozialen Netzwerk?
    - Welche E-Mail-Adressen nutze ich und wie lange schon?
  - Server können als Quelle für **Spam**-Versender dienen.
  - Mögliche **Verstöße gegen die Informationelle Selbstbestimmung** durch missbräuchlich erstellte Schlüssel.
  - **Keine Kontrolle**, welche Signaturen einem Schlüssel hinzugefügt werden.

# KEYSIGNING-PARTIES

- Veranstaltung, durch die das **Web of Trust** durch gegenseitiges Prüfen und Signieren öffentlicher Schlüssel ausgebaut wird.
- **Identifikation einer Person** geschieht meist durch amtliche Dokumente (Personalausweis, Reisepass oder Führerschein).
- **Prüfung des öffentlichen Schlüssels** geschieht durch genaue Betrachtung dessen Fingerabdrucks (z.B. `B65F 4056 8788 AC10 9ED1 9E8F 2170 5CA9 F666 7825`).
- Aus **Sicherheitsgründen** wird häufig nicht vor Ort signiert.
- Verbreitet sind Keysigning-Parties v.a. bei Universitäten, diversen IT-Messen, dem CCC und natürlich den Piraten. ;)

# DIE BENÖTIGTEN WERKZEUGE

- Freies Open Source-E-Mail-Programm **Mozilla Thunderbird**.
- Mozilla Thunderbird-Add-on **Enigmail**.
  - Erweiterung zum Verschlüsseln/Signieren elektron. Nachrichten.
  - Als Voraussetzung muss GnuPG installiert sein.
  - GNU/Linux-Benutzer sollten das Add-on aus ihrer Paketverwaltung installieren.
- Freie Implementierung des OpenPGP-Standards **GnuPG**.
  - GNU/Linux: In der Regel bereits vorinstalliert.
  - Mac OS X: **GPGTools**
  - Windows: **Gpg4win**

# WAS NOCH ZU BEACHTEN WÄRE

- **Sicherheit** der Kommunikation kann unterminiert werden.
  - **Kompromittierung** des eigenen Systems durch Trojaner oder Hintertüren in Software (z.B. in proprietären Betriebssystemen).
  - Fortschritte in der **Kryptoanalyse**.
- **Metadaten** (u.a. die Adressen des Senders und Empfängers, Betreff oder Zeitpunkt der Kommunikation) werden unverschlüsselt übertragen.
- Analyse und Speicherung der **Metadaten** möglich.
- Auswertung der **Schlüssel-Server**.
- Verschlüsselte Kommunikation ist als solche erkennbar und kann eine Person **verdächtig** werden lassen.

# WAS NOCH ZU BEACHTEN WÄRE

- Am 18.10.07 hat der **Bundesgerichtshof** jedoch in seinem Urteil Az.: StB 34/07 eindeutig festgestellt, dass Verschlüsselung als Tatverdacht nicht ausreichend ist.
- In bestimmten Ländern kann der Einsatz von Verschlüsselung **illegal** sein oder man kann zur Herausgabe der Schlüssel gezwungen werden (z.B. Großbritannien).
- Vollständig **anonyme Kommunikation** ist praktisch unmöglich.
- Fällt der **private Schlüssel** in fremde Hände, kann die gesamte vergangene Kommunikation entschlüsselt werden.

# WAS NOCH ZU BEACHTEN WÄRE

- **E-Mail-Programme** können im Hintergrund Entwürfe einer aktuell bearbeiteten Mail speichern. Im Falle des IMAP-Protokolls kann somit der Klartext einer Mail auf einen Server des Mail-Anbieters gelangen! Darum am besten automatisches Speichern abstellen.
- **Mozilla Thunderbird/Enigmail** ist von Haus aus jedoch so konfiguriert, dass Nachrichtenentwürfe grundsätzlich verschlüsselt abgelegt werden. 

- Einen Blick auf **OpenPGP Best Practices** werfen.

# FAZIT

- Die **Ende-zu-Ende-Verschlüsselung** bzw. die damit verbundenen Verfahren, die hinter OpenPGP stecken, sind **derzeit noch sicher**.
- Wie gesehen lauern im Bezug auf OpenPGP allerdings auch einige **Fallstricke**.
- Im Schatten der Snowden-Veröffentlichungen brüten derzeit viele Hacker und Kryptoexperten über **neue Möglichkeiten der sicheren und anonymen Kommunikation**.

# DISCLAIMER

- Dieser Vortrag enthält Vereinfachungen.
- Er ist nach bestem Wissen und Gewissen erstellt, kann aber Fehler enthalten und erhebt deshalb keinen allgemeinen Wahrheitsanspruch.
- Fragt und forscht im Zweifelsfall selbst nach. Die Verantwortung liegt bei Euch.

# FRAGEN?

# QUELLEN

- Asymmetrisches Kryptosystem
- Enigmail (OpenPGP-Add-on für Thunderbird, benötigt GnuPG, z.B. in Gpg4win enthalten)
- GNU Privacy Guard (GPG)
- GnuGP (GNU Privacy Guard – freie Implementierung des OpenPGP-Standards)
- Gpg4win (GNU Privacy Guard für Windows)
- GPGTools (GNU Privacy Guard für Mac OS X)
- Hybride Verschlüsselung
- Keysigning-Party
- Mozilla Thunderbird (weit verbreitetes Open-Source-E-Mail-Programm)
- OpenPGP
- OpenPGP Best Practices
- Pretty Good Privacy (PGP)

# QUELLEN

- Schlüsselserver
- Symmetrisches Kryptosystem
- Thunderbird Mail DE - Enigmail OpenPGP (gute Enigmail-Dokumentation)
- Vortrag „PRISM BREAK“ von André Martens (Piraten Freiburg) anläßlich einer CryptoParty
- Web of Trust