

CRYPTOPARTY

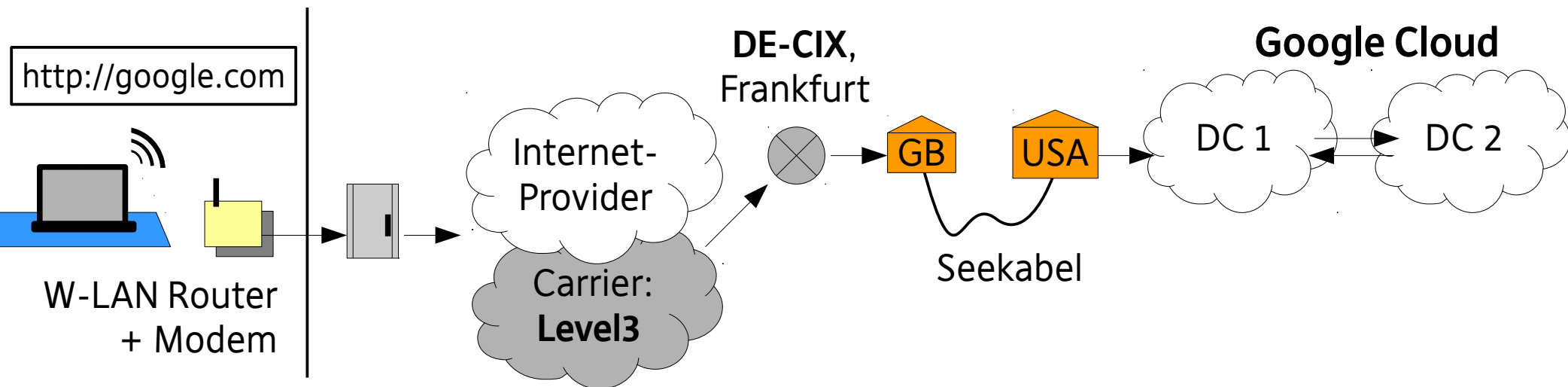
VERSCHLÜSSELUNG

„Encryption works.

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

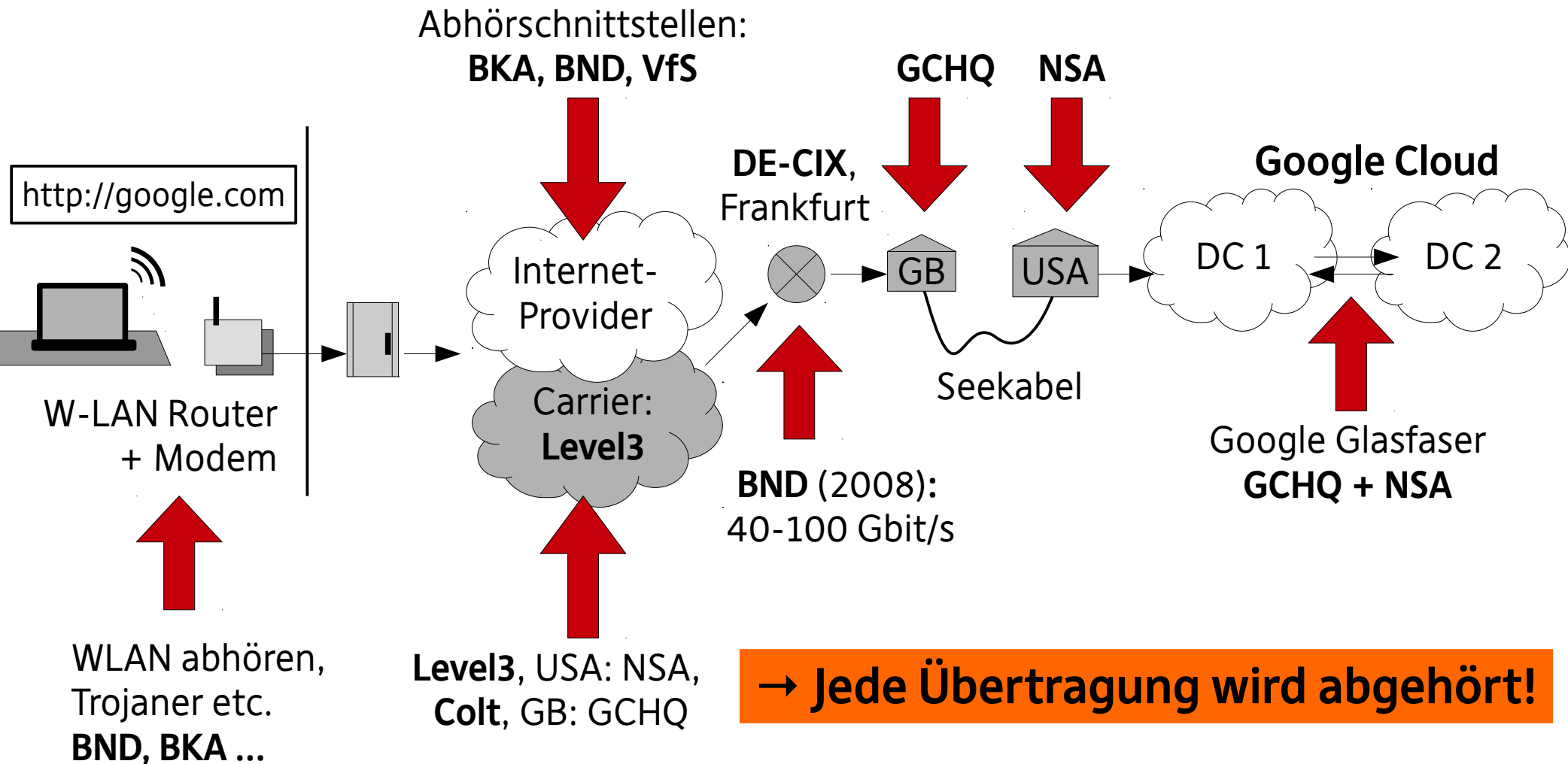
Edward J. Snowden, 17. Juni 2013

WIE FUNKTIONIERT DAS INTERNET UND WIE WIRD ES ABGEHÖRT?

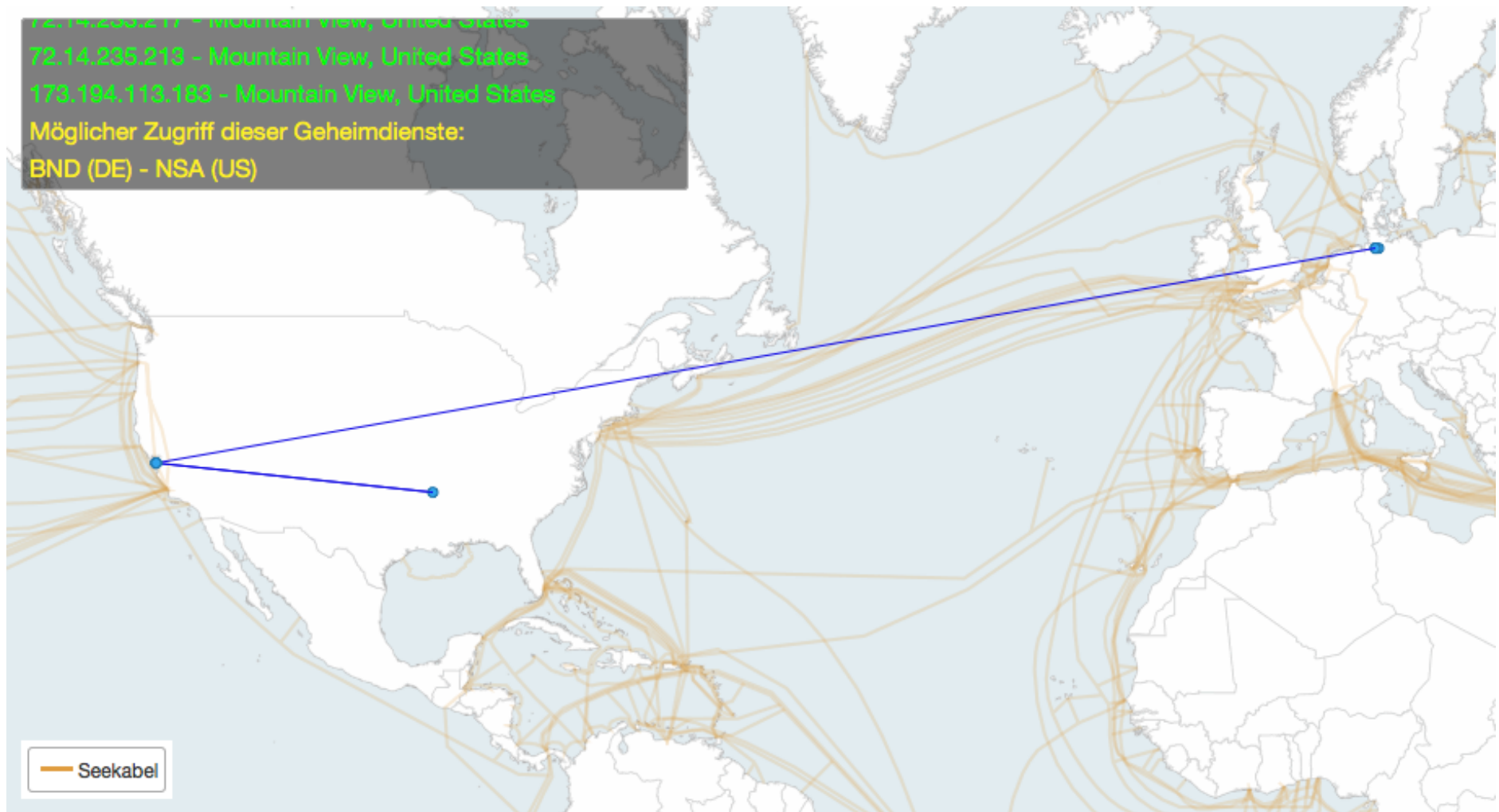


→ Daten bisher meist unverschlüsselt!

WIE FUNKTIONIERT DAS INTERNET UND WIE WIRD ES ABGEHÖRT?



WIE FUNKTIONIERT DAS INTERNET UND WIE WIRD ES ABGEHÖRT?



→ <http://apps.opendatacity.de/prism/de>

WAS IST VERSCHLÜSSELUNG?

- **Verschlüsselung** (Chiffrierung) wandelt mit Hilfe eines **Verschlüsselungsverfahrens** (Chiffre) lesbaren **Klartext** (Dechiffirat) in unleserlichen **Geheimtext** (Chiffirat) um.

- Beispiel

- Klartext: Geheimbotschaft

- Geheimtext:

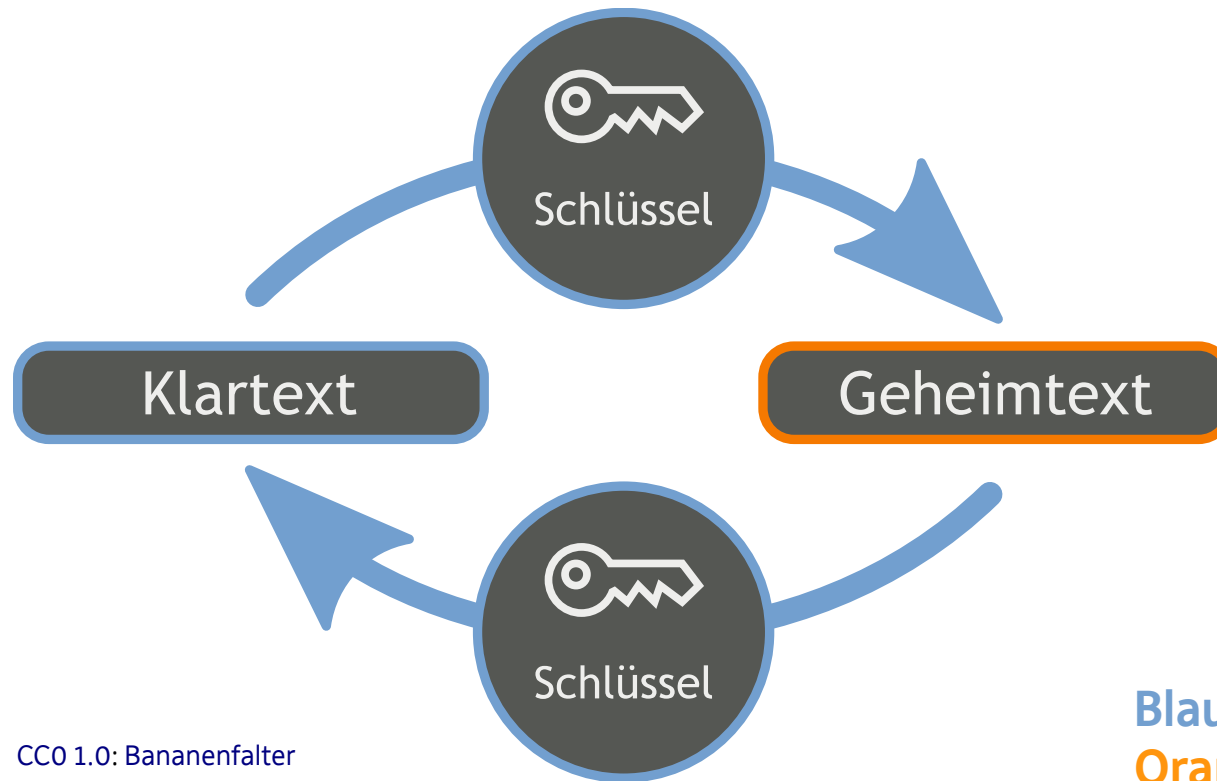
```
hQIMA2f18waqUmWwARAAggev8bFnetgNoVrcUxX0KWF64OAEiGm+ZOmBbHhCU0Ju
McR2H2zkHY1oEpx84qPaGV4zcKLxLpjoypeZavMUFgKedGmHphMzcAs7PsU1lqgK
GgdY7E4FZ8fMAYnTuo78jHxyJ4hi9afjg6JjYcZo11p6IR54R52/uFOCJ6wDfcfo
90Z2v6PgY6H2Cc1PDV4kuZ1UrbIcjQfGmF5ZLbjOy4/c00p5cMUYa8o5hLvkw24s
DDBrdqCQsIYCI9gyrwUZr8xahES4fXI1PX7RwQegAD0rRzxLEJxFdSs4ZkpFwZ/r
PX3b6wO/ON1FZLb3QiPsEdhw99FxVsqxItFz4IS01obZHycsM8bEd5KGTJhBvHv5
pA/KhOGxeKqVEJ5BdOGb4q1qRrmtHpFTQlId1pt+jScr/a/Qy88NryOfBFidftjH
RZr7K3rlq/rQSnegtpUxiDIpAxoMi5ACJjMXyiqm2u6NorVMXEyc/Af7P+1IwQPu
kdDox5Sgb8YkBs3dZKXYX9TvuoyadaAyGQ9SacNReucZqC+7s11koBaa07Lu2EEa
J6RnloHAtMjlKWVxJ8aUofusCKcaKZAax66TMQWgd5FhLpVYDdeUXavz3XkJBoZD
vH5wWfQJNGOgPozNYX4yX2Zd5caWdUclU85ocCTbi/kk6qGneQFMmUlKPDZYUHfS
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.

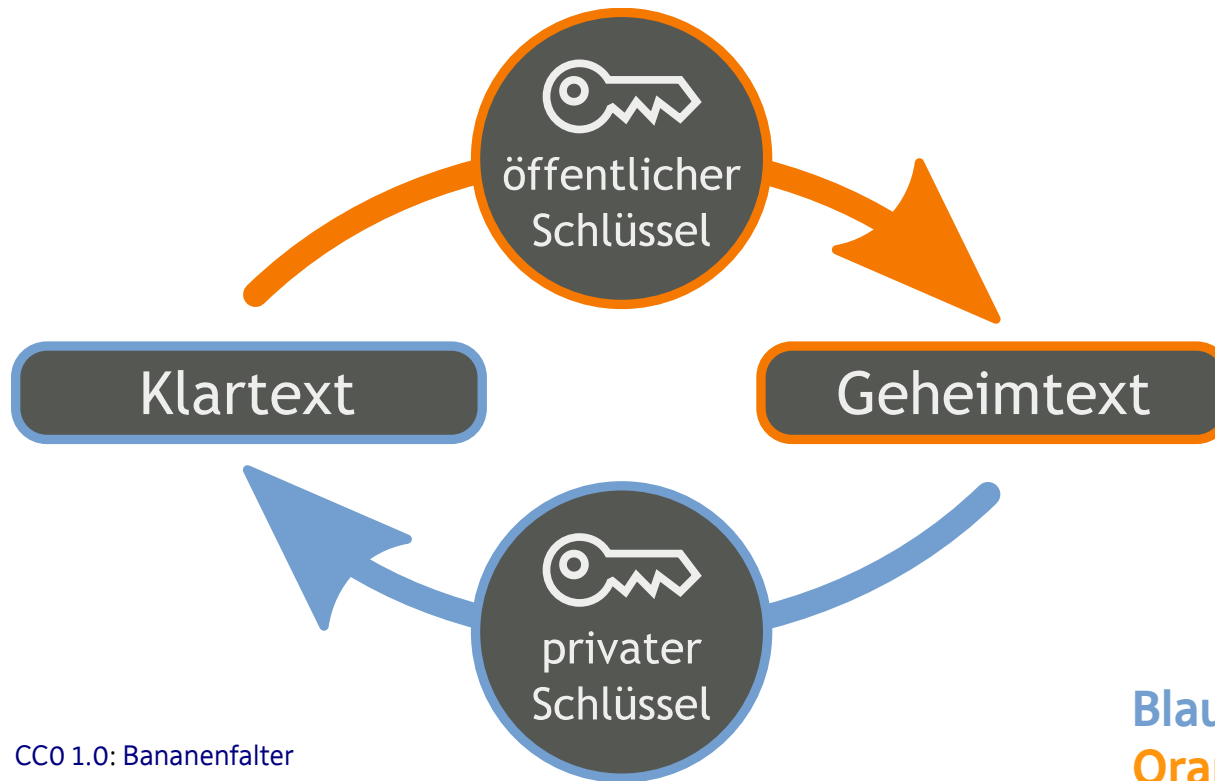


CC0 1.0: Bananenfalter

Blau: geheim
Orange: öffentlich

ASYMMETRISCHE VERSCHLÜSSELUNG

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

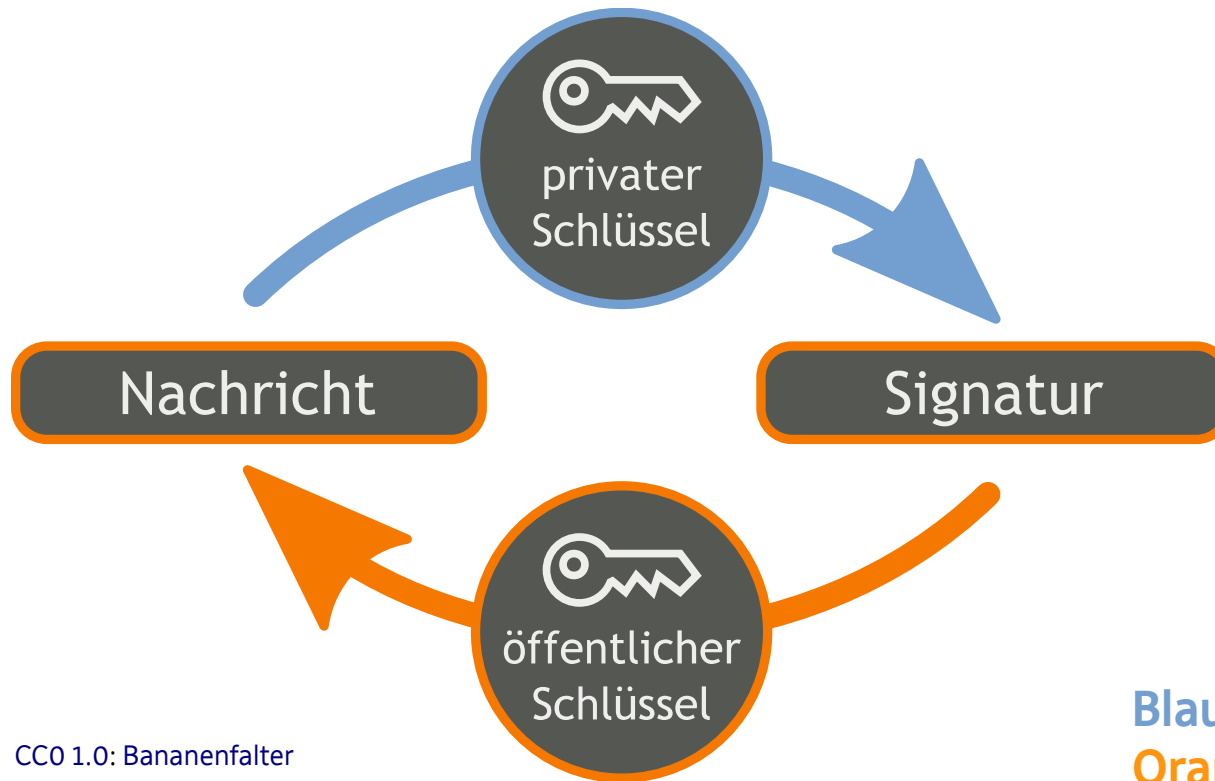


CC0 1.0: Bananenfalter

Blau: geheim
Orange: öffentlich

ASYMMETRISCHE VERSCHLÜSSELUNG

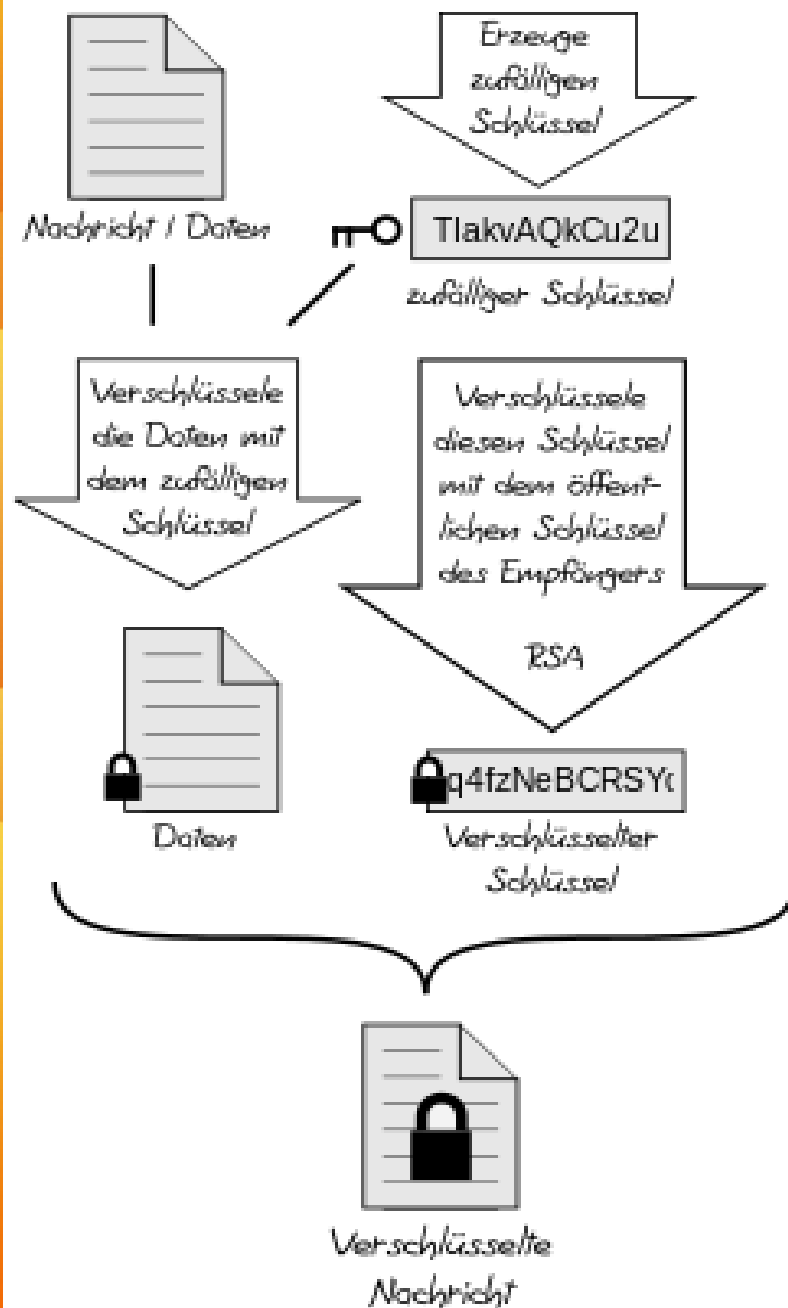
- Mit demselben Schlüsselpaar können Nachrichten auch mit einer **Signatur** versehen bzw. unterschrieben werden, um die Integrität, Authentizität und Verbindlichkeit sicherzustellen.



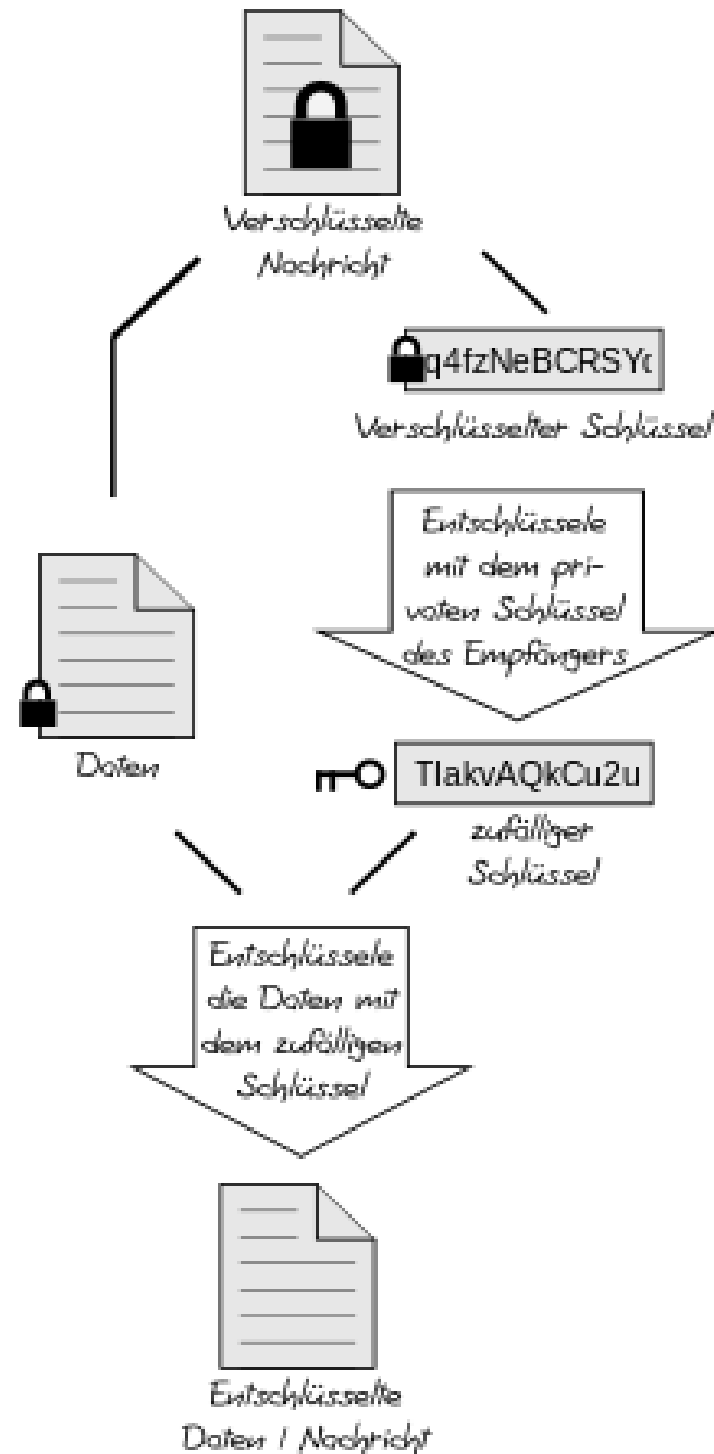
CC0 1.0: Bananenfalter

Blau: geheim
Orange: öffentlich

Verschlüsselung



Entschlüsselung



PGP-TOOLS

- **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.

TOOLS

- **PGP und ähnliche** (Pretty Good Privacy)
 - Weit verbreitet
- **DE-Mail**
 - Und was machen wir in der EU oder weltweit?
- **Volksverschlüsselung / Telekom**
 - Weil PGP zu umständlich sei und für den Laien nicht handhabbar ??
 - Nur in DE, nur mit E-Perso, keine Smartphones, kein Linux oder Mac, kein Webmail

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.

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** (auch für Mail-App)
 - Windows: **Gpg4win**

ANDERE WERKZEUGE

- Webseite <https://encrypt.to>, Beispiel:
 - <https://encrypt.to/thomas.christinck@piratenpartei-stuttgart.de>
-
- Plugin „Mailvelope“ für Firefox und Chrome
 - Verschlüsselt Mails von vielen Webmailern
 - Schlüssel bleiben beim Client
 - Verbesserte Version von 1&t1/Web.de:
mehrere Endgeräte, Mobile Apps