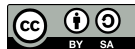
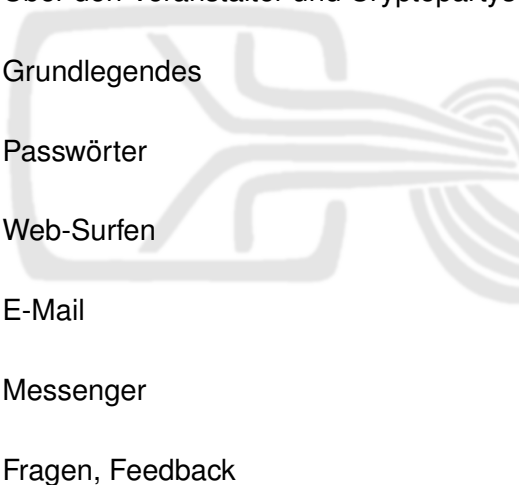


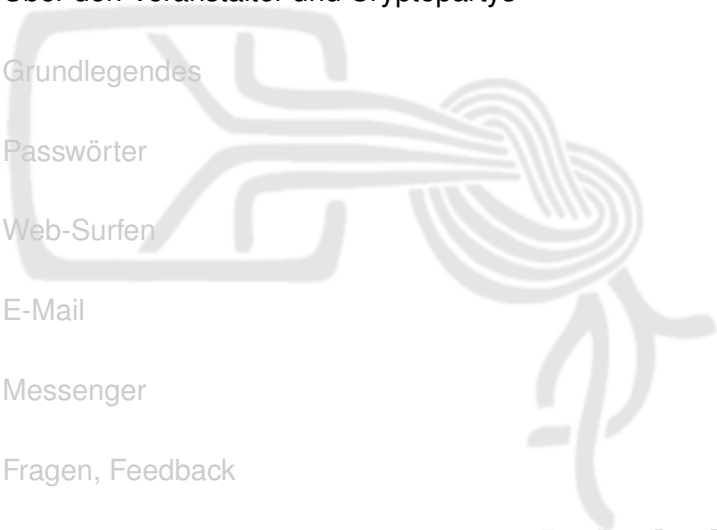
# Cryptoparty

Michael Weiner, Florian Wilde

22. April 2017

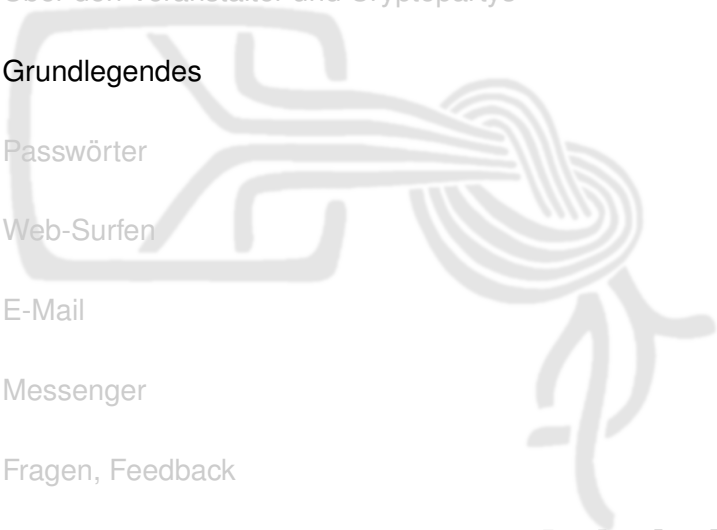


- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback
- 

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback
- 

- Chaos Computer Club München e.V.
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
- Medienzentrum München (MZM)  
Institut für Medienpädagogik in Forschung und Praxis  
JFF – Jugend Film Fernsehen e.V.

- Weltweite Bewegung von technisch interessierten
- Ziel: Datensicherheit für jedermann
- Themen sind z.B.
  - Kommunikation: E-Mail, Anrufe, Chat
  - Datenspeicherung und -weitergabe
  - Veröffentlichen von Informationen
  - Passwörter
- Aus Zeitgründen beschränken wir uns heute auf
  - Passwort-Management
  - Anonyme(re)s Web-Surfen
  - E-Mail-Verschlüsselung und -Signatur
  - ... und mehr auf Anfrage, wenn noch Zeit ist

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes**
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback
- 

- 100% Sicherheit gibt es nicht
- Absichern heißt, Angriffe *teurer* zu machen
  - Die Kosten für den Angriff müssen den Wert der Daten übersteigen
  - Ein Angriff darf sich nicht mehr *lohnen*
  - Problem: Wert wird oft unterschätzt
- Was wir hier zeigen, ist ein Anfang
  - Hilft dagegen, als „Beifang“ zu enden
  - Gegen gezielte Angriffe – auch durch Verwechslung – benötigt es deutlich mehr
- Irren ist menschlich – auch was die Inhalte der folgenden Folien betrifft :-)

- *Was* soll sichergestellt werden?
  - Eigene Anonymität
  - Echtheit des Gegenübers (Authentizität)
  - Unverfälschtheit der Nachricht (Integrität)
  - Geheimhaltung der Nachricht (Vertraulichkeit)
  - ...
- *Wem* vertraut Ihr?



## Woher weiß man, wem man vertrauen kann?

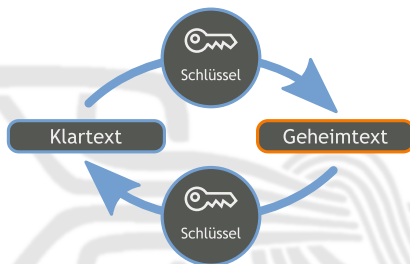
- Kurze Antwort: weiß man *nicht*
- Lange Antwort
  - es gibt Fragen, die man stellen kann...
  - ... und es gibt das Bauchgefühl

Beispiel: *Wo* sind meine Daten?

- Auf einem Blatt Papier zuhause in meiner Schublade.
- Auf meinem Computer:
  - Wie gut ist die Software *überprüfbar*, die meine Daten verwaltet?
    - Open Source (in menschenlesbarer Form öffentlich): gut überprüfbar
    - Closed Source (menschenlesbare Form geheim): quasi nicht überprüfbar
- In der Cloud
  - *Wer* betreibt einen Dienst?
  - Womit *verdient* der Betreiber sein *Geld*?
  - Wem könnten die Daten *nutzen* oder *schaden*?
  - Was *lernt* der Betreiber über mich?

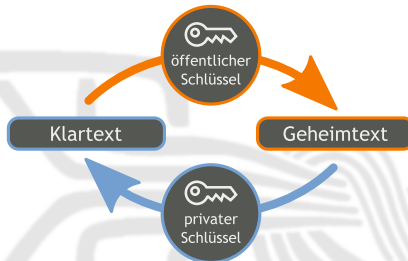
- Meta-/Verbindungsdaten (“Briefumschlag”)
  - Absender, Empfänger, Betreff einer E-Mail
  - Besuch und Aufenthaltsdauer auf einer Webseite
  - Wer, wann, wie lange mit wem telefoniert
  - Aufenthaltsort von Mobiltelefonen: Bewegungsprofil!
- Nutz-/Inhaltsdaten (“Brief”)
  - E-Mail-Text und -Anhänge
  - Webseiten-Inhalte
  - Gesprochene Sprache beim Telefonieren
  - SMS-Inhalt

Metadaten zu verschlüsseln ist nicht möglich,  
sie zu verschleiern schwierig.



- Jahrtausende altes Konzept
- *Ein* Schlüssel zum Ver- und Entschlüsseln, den *alle* Beteiligten kennen
- Problem: Schlüsselaustausch
  - Wer den Schlüssel kennt, kommt auch an die Daten
  - Wer den Schlüssel kontrolliert, kontrolliert die Daten
    - Ransomware

# Asymmetrische Kryptographie

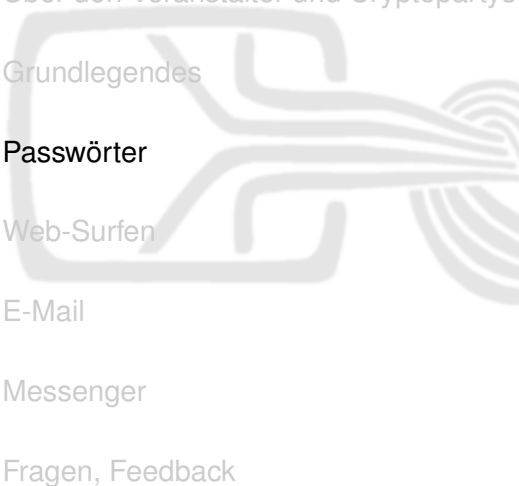


- Prinzip: Schlüssel besteht aus einer *privaten* und einer *öffentlichen* „Hälfte“
  - Öffentlichen Teil darf/muss man weitergeben
  - Privaten Teil muss man unbedingt geheim halten
- Wird verwendet, um vertraulichen Kanal aufzubauen
- Problem weiterhin: Authentizität des öffentlichen Teils

Bildquelle: „Asymmetrisches Kryptosystem mit Verschlüsselung und Entschlüsselung“ von Bananenfalter / CC0

- Verschlüsselung
  - Absender *verschlüsselt* mit *öffentlichem* Teil des *Gegenübers*
  - Nur Gegenüber kann mit *privatem* Gegenstück *entschlüsseln*
- Digitale Signatur
  - Absender unterschreibt mit *eigenem privaten* Teil
  - Jeder kann mit *öffentlichem* Gegenstück *überprüfen*

Es ist mathematisch komplex und benötigt Jahrtausende, um aus einer Signatur oder dem öffentlichen Teil den privaten Teil zu berechnen

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter**
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback
- 

Wer hat mindestens fünf Online-Accounts?



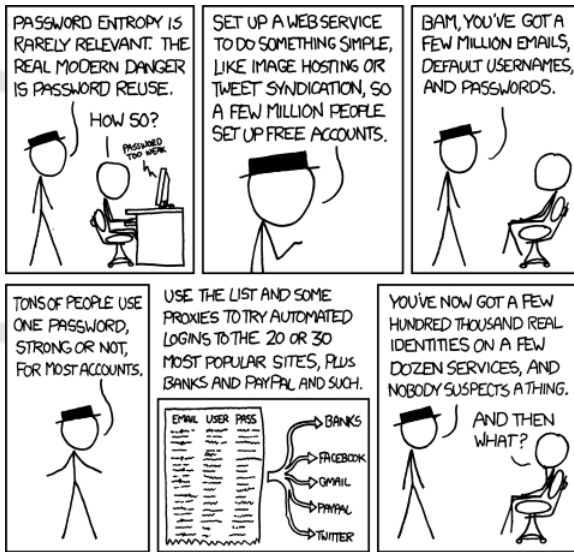


Wer hat mindestens fünf Online-Accounts?  
Wer hat dafür mindestens drei verschiedene Passwörter?

Wer hat mindestens fünf Online-Accounts?  
Wer hat dafür mindestens drei verschiedene Passwörter?  
Wer beachtet, Passwörter nur über HTTPS einzugeben?

- Kundendaten gehen häufig verloren
  - Schaden lässt sich begrenzen, wenn Benutzername und Passwort nur bei diesem einen Anbieter passen
- Besonders wichtig: E-Mail-Accounts
  - Weil „Passwort zurücksetzen“ oft via E-Mail
  - Wer den E-Mail Account übernommen hat, kann dadurch sämtliche Accounts übernehmen
- Ideal: Jedes Passwort nur einmal verwenden
- Alternative: Passwörter „salzen“
  - *passwort.amz* für Onlineshop a
  - *passwort.zal* für Onlineshop z
  - *anderesspasswort* für Mails

# Password Wiederverwertung



## Anforderungen

- Klein- und Großbuchstaben, Zahlen, begrenzt: Sonderzeichen
- Wichtiger: Lang genug!

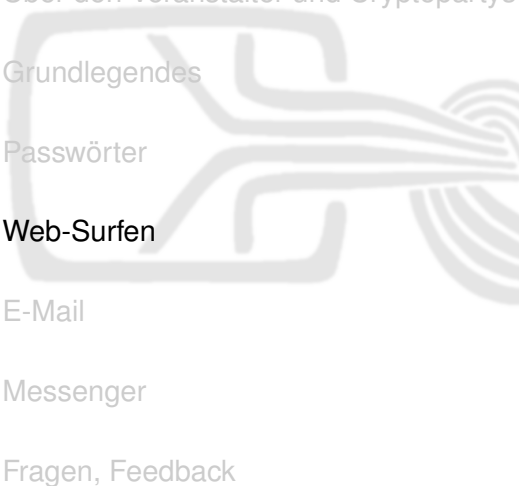
## Merkbarkeit

- Geschichte dazu ausdenken
- Melodie und Rhythmus rein bringen
  - Gehirn kann sich Melodien besonders leicht merken
  - Ermöglicht schnelles Eintippen
    - Längere Passwörter sind weniger nervig
    - Passwort mitlesen ist schwieriger

- Software zur Verwaltung von Passwörtern
- Kann automatisch komplexe Passwörter erzeugen
- Datenbank wird mit Master-Passwort verschlüsselt
  - Anzahl der zu merkenden Passwörter geringer
- Beispiele
  - KeePassX (Open Source)
  - KeePass (Open Source)

**Achtung:** Unsichere Update-Prüfung vor Version 2.34
- *Wichtige Passwörter trotzdem merken oder an einem sicheren Ort aufbewahren!*

# Fahrplan

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen**
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback
- 

- Cookies und Co (HTML5 Persistent Local Storage, Flashcookies, ...)
- Browser-Fingerabdruck
- IP-Adresse

Jede Website und jedes Werbenetzwerk kann Personen und Computer (wieder-)erkennen

## Tools zur Aufklärung

- EFF: Panoptlick
- Wired: Datenblumen



# Schutzmaßnahmen – Level 1

Nur Einstellungen ändern

- Standardsuchmaschine auf datenschutzfreundliche Anbieter ändern, z.B.
  - DuckDuckGo
  - Startpage
- Cookies verbieten, nur selektiv erlauben
  - Firefox: about:preferences
- Plugins auf „Click-to-use“ stellen
  - Firefox: about:addons

Eventuell:

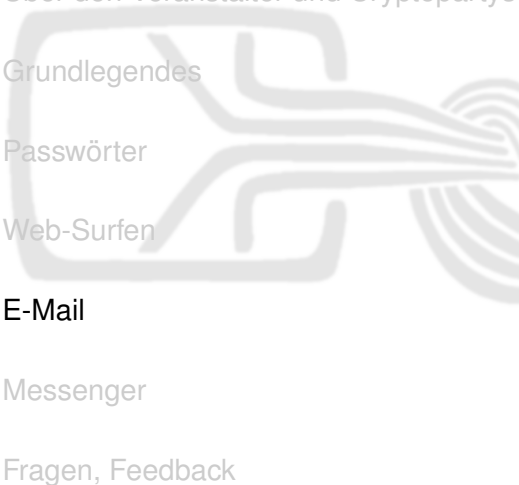
- Blockierung von „bösen“ Webseiten abschalten
- Statusberichte des Browsers abschalten

- Adblocker –  
Schadsoftware immer öfter über Werbeanzeigen!
  - uBlock origin
    - Keine „acceptable adds“ wie bei Adblock Plus
    - Blockiert auch andere nervige Dinge außer Werbung
  - EFF: Privacy Badger
    - Blockiert anhand von Verhalten, nicht Listen
- NoScript
  - Erlaubt gezieltes ein-/ausschalten von Java, JavaScript etc.
- EFF: HTTPS-Everywhere
  - Nutzt automatisch HTTPS, falls von Seite unterstützt
  - Benutzt lokale Liste der Seiten, keine Online-Abfrage
- RefControl
  - HTTP-Referrer = von welcher Seite komme ich

# Schutzmaßnahmen – Level 3

Neue Programme installieren oder benutzen

- Tor Browser Bundle (Freie Software)
  - Anonymisierung des Netzwerkverkehrs durch „intelligente Umwege“
  - Fingerabdruck bei allen Tor Browsern identisch
  - Hohe Sicherheit, aber prinzipbedingt langsamer
- Tails (Freie Software)
  - Abgesichertes Betriebssystem inkl. Tor
  - Live System = kann direkt von CD gebootet werden hinterlässt keinerlei Spuren am PC

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail**
  - 6 Messenger
  - 7 Fragen, Feedback
- 

# E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man

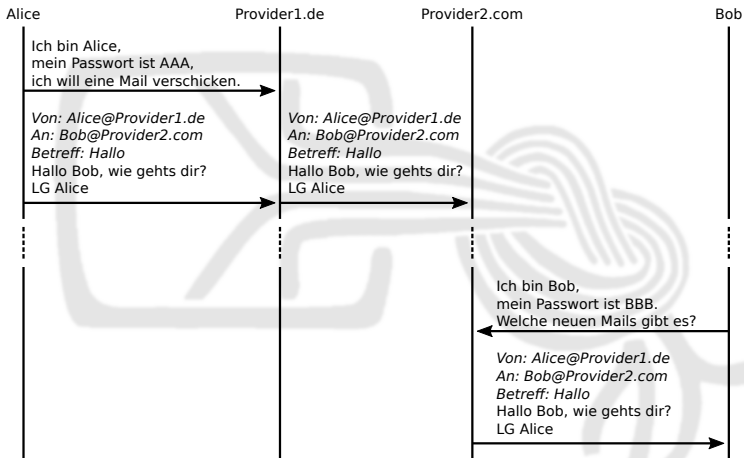
- die Vertraulichkeit (das „Briefgeheimnis“) umsetzt  
⇒ Verschlüsselung
- die Echtheit des Gegenübers sicherstellt  
⇒ Digitale Signatur

Außerdem:

- Wie man sicherstellt, dass sein E-Mail-Passwort nicht einfach mitgelesen werden kann

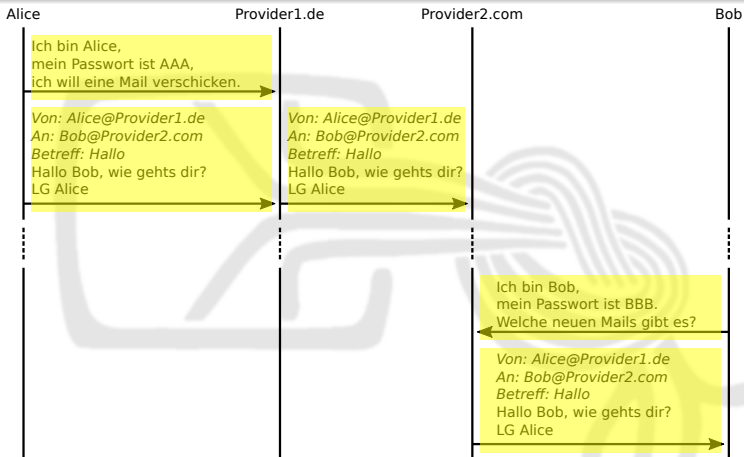
# E-Mail

## Funktionsweise



# E-Mail

## Transportverschlüsselung (SSL/TLS bzw. STARTTLS)

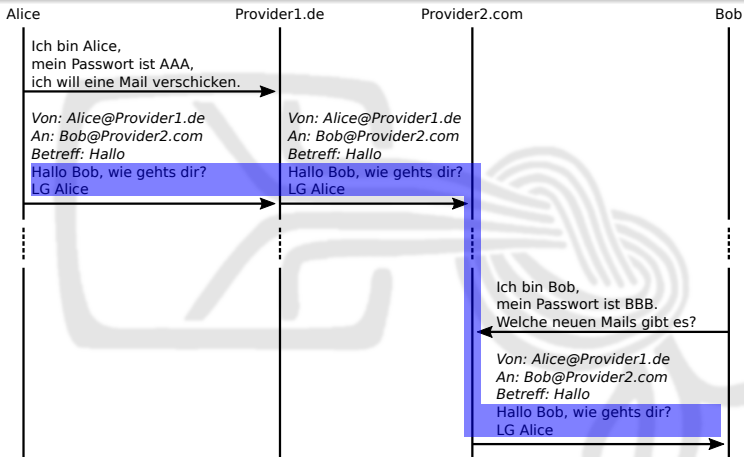


Transportverschlüsselung

- muss von den Mailanbietern unterstützt werden
- Konfiguration des Mailprogramms überprüfen!

# E-Mail

## Ende-zu-Ende-Verschlüsselung (OpenPGP, S/MIME)



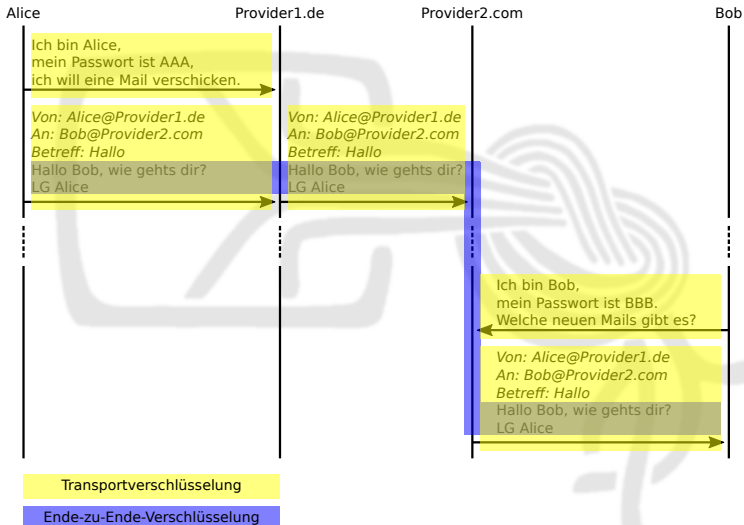
### Ende-zu-Ende-Verschlüsselung

- unabhängig vom Mailanbieter möglich
- benötigt Zusatzsoftware und Schlüssel bei beiden Kommunikationspartnern



# E-Mail

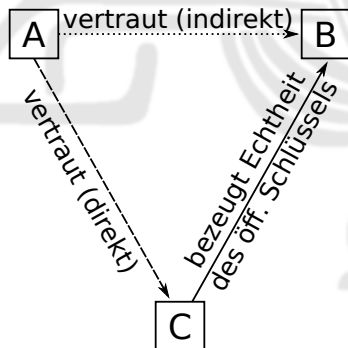
## Kombination Transport- und Ende-zu-Ende-Verschlüsselung



# Authentizität öffentlicher Schlüssel

Was, wenn A eine Nachricht an B schicken will,  
aber den öffentlichen Schlüssel von B nicht kennt?

- 1 Im "Telefonbuch" nach dem Schlüssel suchen
- 2 Echtheit mit Hilfe eines *vertrauenswürdigen Dritten C* überprüfen



# Wie stellt man Vertrauen in öffentliche Schlüssel her?

- S/MIME – Hierarchischer Vertrauensansatz
  - hier nicht behandelt
- OpenPGP – Dezentraler Vertrauensansatz
  - jeder kann festlegen, wem er vertraut
    - er kann die Echtheit eines Schlüssels z.B. bei einem persönlichen Treffen überprüfen
  - jeder *kann* sein Vertrauensnetz veröffentlichen (Web-of-Trust)
    - Vorteil: Man kann “Freunden von Freunden” vertrauen
    - Nachteil: Beziehungen zwischen Menschen öffentlich  
Aber: Facebook sagt da viel mehr aus

# Welche Software benötigt man?

## OpenPGP Backend

Macht die eigentliche Ver-/Entschlüsselung & Signatur

Linux:	Windows:	Android:
<i>on-board</i>	GPG4Win	OpenKeychain

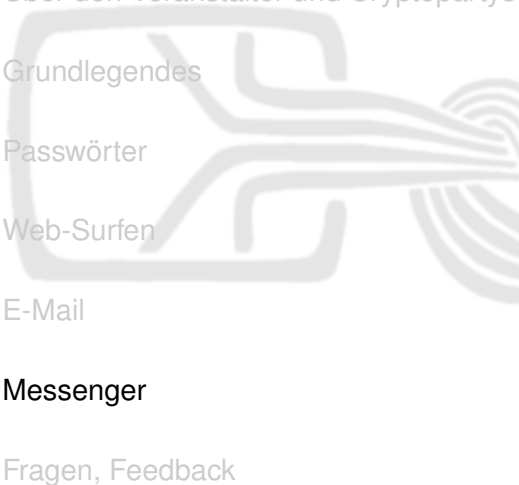
## Plug-In fürs Mailprogram

Grafische Oberfläche, leichtere Schlüsselverwaltung, etc.

Thunderbird:	Outlook:	K9-Mail:
Enigmail	GPG4Win	—

# Nächste Schritte:

- ❶ Software installieren (siehe vorige Folie)
- ❷ Installationsassistent starten
  - ❶ Schlüsselpaar erzeugen
  - ❷ Passwort festlegen  
(schützt privaten Schlüssel auf der Festplatte)
  - ❸ Identitäten hinzufügen  
(für welche E-Mail-Adresse(n) der Schlüssel gilt)
  - ❹ Widerrufs-zertifikat auf USB-Stick speichern
  - ❺ Öffentlichen Schlüssel auf Keyserver hochladen
- ❸ Erste verschlüsselte und signierte E-Mail schicken :)

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger**
  - 7 Fragen, Feedback
- 

# Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail



- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

Wer benutzt

- WhatsApp



- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

### Wer benutzt

- WhatsApp
- Telegram

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

### Wer benutzt

- WhatsApp
- Telegram
- Threema

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

### Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

### Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal
- Jabber

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

## Bestandsaufnahme

### Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal
- Jabber
- Matrix

- Geschlossene Systeme: WhatsApp & Co
  - App-Entwickler  
ist Dienstanbieter  
und Herr über die “technische Sprache” (das Protokoll)
  - Auswahl eines Dienstes  
bestimmt erreichbaren Personenkreis
  - meist Closed Source
- Offene Systeme (z.B. Jabber/XMPP, Matrix)
  - App-Entwickler, Dienstanbieter und  
Protokoll-Standardisierer sind unterschiedliche Personen
  - App und Anbieter frei wählbar
  - meist Open Source

## WhatsApp

- + Nutzdaten werden verschlüsselt
- + Android: Verwendbar ohne Google Play
- Closed Source
- Anbieter erhält eine Kopie des vollständigen Telefonbuchs (nicht nur WhatsApp-Kontakte)

**Tipp:** Wer sein Telefonbuch nicht freigeben will, kann den Zugriff darauf verweigern (Android: ab Version 6).

Der Nutzungskomfort ist dadurch eingeschränkt.

## Signal

- + Nutzdaten werden verschlüsselt
- Android: Nicht verwendbar ohne Google Play
- Anbieter erhält eine Kopie des vollständigen Telefonbuchs (nicht nur Signal-Kontakte)



## Telegram

- + „Verschlüsselte Chats“ möglich
- Anbieter erhält eine Kopie des vollständigen Telefonbuchs
- Verschlüsselung standardmäßig nicht aktiv
- „Normale Chats“ werden im Klartext auf den Servern gespeichert

## Threema

- + Chats verschlüsselt
  - + komfortabler Schlüsselaustausch über QR-Code
  - + Synchronisation des Telefonbuchs ist optional
  - Closed Source
- kostenpflichtig

## Jabber/XMPP

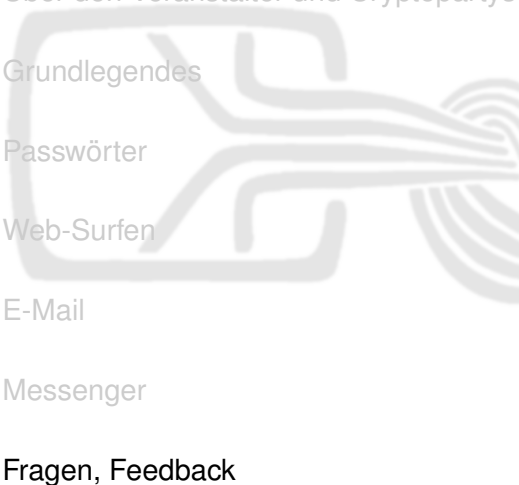
- + Offenes System: Anbieter und App frei wählbar
  - + Verschlüsselung möglich (OTR oderOMEMO)
  - + keine Telefonbuch-Synchronisation vorgesehen
  - Crypto nicht ganz so nutzerfreundlich wie bei kommerziellen Anbietern (aber dafür sind wir ja alle hier :-)
- 
- Apps: Conversations, pidgin, gajim, ...
  - Anbieter: Unis, Hackerspaces, CCC, jabber.org, ...

## Matrix

- + Offenes System: Anbieter frei wählbar
- + Verschlüsselung möglich
- + Telefonbuch-Synchronisation nicht zwingend
- + Anbindung an Drittsysteme möglich (IRC, Skype, ...)
- Hintergrund/Historie der Entwickler umstritten

- Wer auf bestimmten Messenger nicht verzichten kann: Zugriff auf Kontakte verbieten!
- Weitere Infos: EFF Secure Messaging Scorecard  
<https://www.eff.org/secure-messaging-scorecard>  
(gerade in Überarbeitung, alte Version noch verlinkt)

# Fahrplan

- 1 Über den Veranstalter und Cryptopartys
  - 2 Grundlegendes
  - 3 Passwörter
  - 4 Web-Surfen
  - 5 E-Mail
  - 6 Messenger
  - 7 Fragen, Feedback**
- 

- Her damit!
- Fragen an alle Helfer (bitte gebt Euch zu erkennen :-)
- Links: <https://muc.pads.ccc.de/cryptoparty>