

# Verschlüsselung

# Inhalt

- Warum Verschlüsseln?
- Sichere Passwörter
- Meinen Computer verschlüsseln
- Meine Kommunikation verschlüsseln
  - Email
  - Instant-Messaging
- Weitere Infos und Hilfe

# Warum Verschlüsseln?

- PC gerät in falsche Hände
  - verloren
  - geklaut
  - beschlagnahmt
- Mails und Chats
  - Internetverkehr abhören

# Passwörter

- keine Wörter aus dem Lexikon
- für „kritische“ Dienste verschiedene Passwörter wählen
- Sonderzeichen, Zahlen, groß/klein
- mindestens 10 Zeichen

2516 - 123456

2188 - password

1205 - 12345678

696 - qwerty

498 - abc123

459 - 12345

441 - monkey

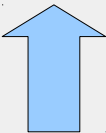
413 - 111111

385 - consumer

376 - letmein

# Passwörter

Beispiel:

u#5s \_\_\_\_\_ +o\$3  


Jeden 2. Buchstaben in der URL von hinten gelesen (ohne TLD und Subdomains)

- Passwort für *gmail.com*: u#5s**lag**+o\$3
- Passwort für *paypal.de*: u#5s**lpa**+o\$3
- Passwort für *ebay.de*: u#5s**yb**+o\$3

## 3 Herangehensweisen:

- Container
- Home-Verzeichnis
- Komplett

# Container

- Datei, die eine verschlüsselte Ordnerstruktur enthält
  - Passwortabfrage bei Zugriff
  - wird im System wie ein USB-Stick angezeigt
- 
- ✓ einfach
  - ✓ portabel
  - x Zugriff hinterlässt Spuren im System
  - x sinnvoll für unabhängige Programme / Dokumente

# Home-Verzeichnis

- ausschließliches Verschlüsseln eigener Dateien
  - beim Anmelden werden automatisch alle Dateien des Nutzers entschlüsselt
  - nur unter Linux möglich
- 
- |  |   |
|--|---|
| ✓ einfach                                    | ✗ kritische                                   |
| ✓ keine zusätzliche<br>Passworteingabe nötig | Systeminfrastruktur<br>bleibt unverschlüsselt |
|  | ✗ Benutzer muss neu<br>angelegt werden        |



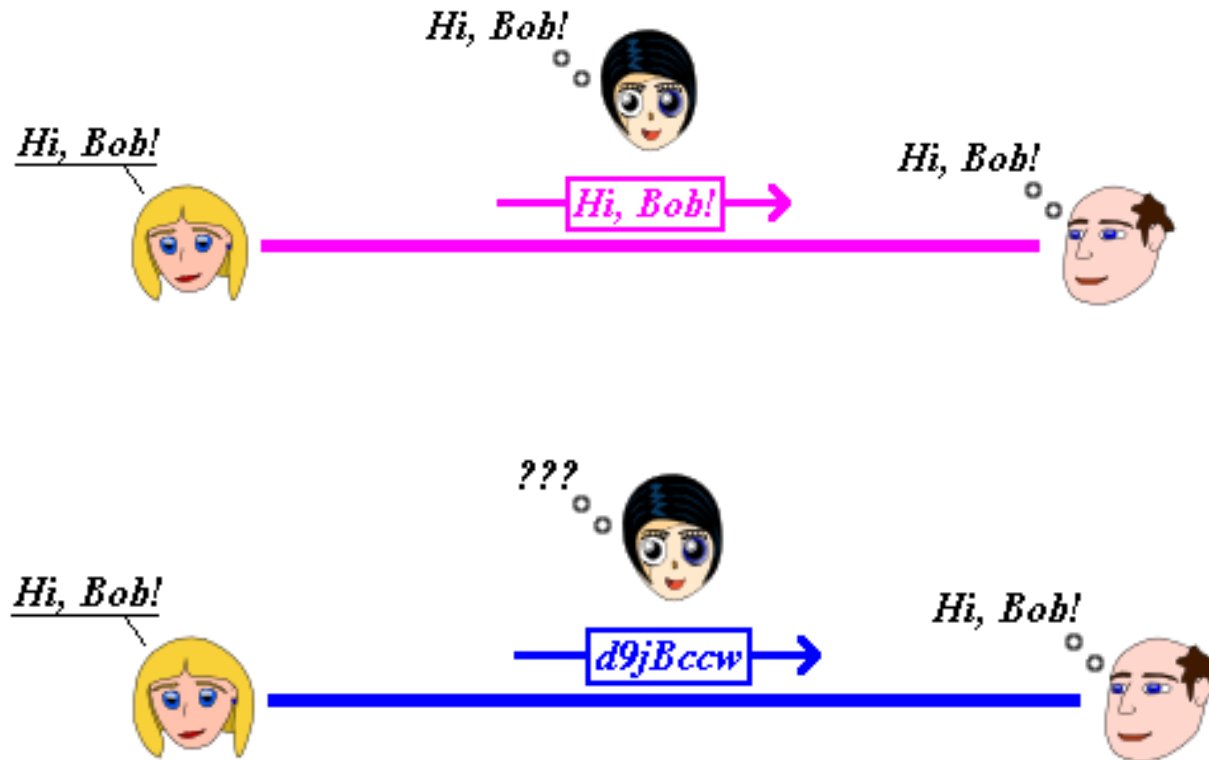
# Komplett-Verschlüsselung

- Verschlüsselung des gesamten Systems
  - Passwortabfrage vor dem Starten des Systems
- 
- |  |  |
|--|--|
| ✓ Ohne Passwort kein Zugriff auf Systemdateien | ✗ Problematisch bei Mehrbenutzersystemen |
|--|--|

# Festplattenverschlüsselung

- vormals Unverschlüsseltes sollte 1x überschrieben werden, bevor es verschlüsselt wird (*“Wipe”*)
- Standard-Tools kommen mit empfehlenswerten Default-Einstellungen

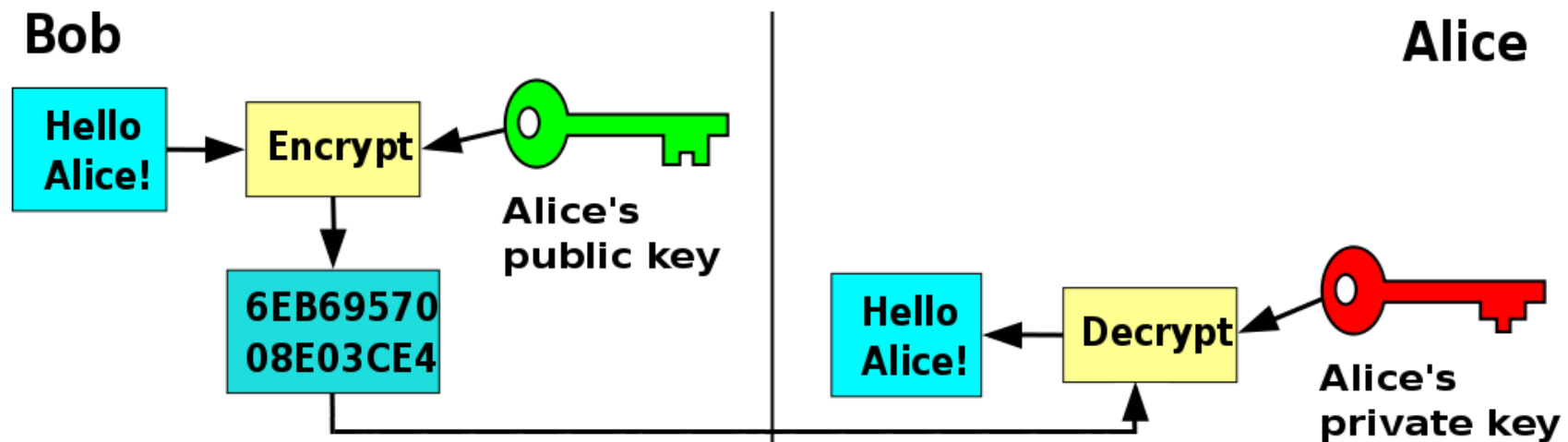
# Verschlüsselte Kommunikation



<http://www.cypherpunks.ca/otr/>

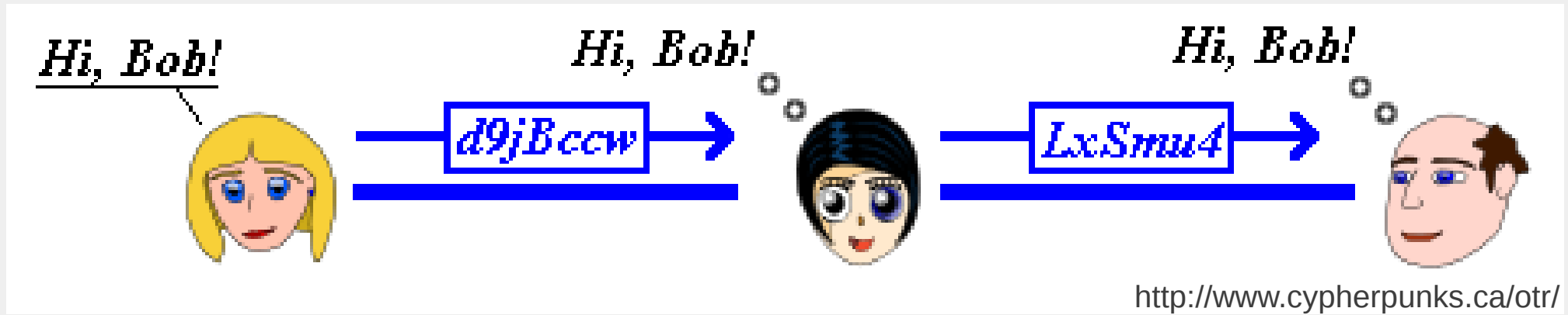
# Asymmetrische Verschlüsselung

- **Privater Schlüssel** entschlüsselt
  - muss geheim gehalten werden
- **Öffentlicher Schlüssel** verschlüsselt
  - wird öffentlich an jeden verteilt



[http://de.wikipedia.org/w/index.php?title=Datei:Public\\_key\\_encryption.svg&filetimestamp=20060821211116](http://de.wikipedia.org/w/index.php?title=Datei:Public_key_encryption.svg&filetimestamp=20060821211116)

# Authentifizierung



- notwendig, um Gesprächspartner eindeutig zu identifizieren („Man-in-the-middle-Angriff“)
- am besten persönlich
- OTR bietet (je nach Plugin) Geheimfragen/Shared Secrets

Der Aufwand lohnt sich!

# Mail-Verschlüsselung

- Installation
  - **Windows:** Portable Thunderbird downloaden
  - **Ubuntu/Debian:** die Pakete thunderbird und enigmail installieren

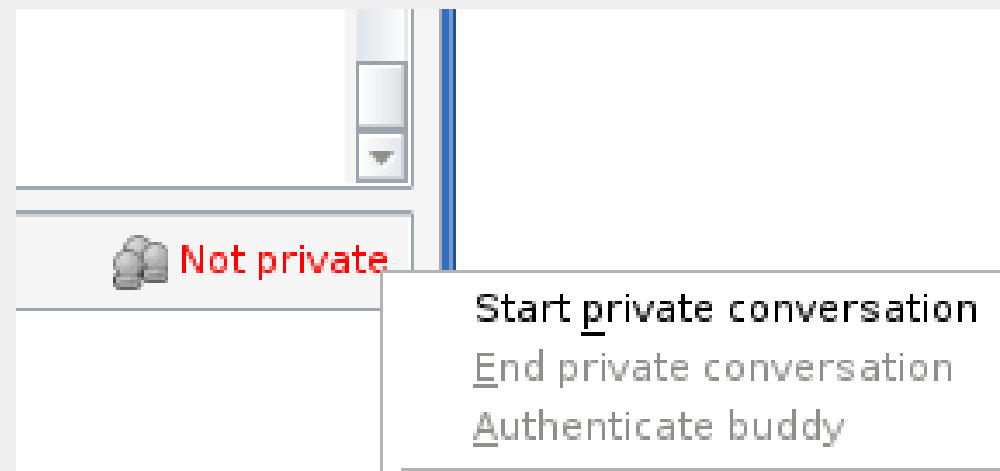
# Instant Messaging: OTR

- OTR-fähige Messenger (mit Plugin):
  - Pidgin (Windows, Linux)
  - Miranda (Windows)
  - Trillian Pro (Windows)

(Adium und einige andere unterstützen OTR ohne Plugin)

# Instant Messaging: OTR

- Installation am Beispiel Pidgin:
  - **Windows:** .exe-Datei
  - **Ubuntu:** Paket pidgin-otr
  - Plugin aktivieren, Schlüssel per Klick erzeugen
  - Im Gesprächsfenster lässt sich eine private Unterhaltung starten





# Chat

- Installation
  - **Windows:** Portable Pidgin downloaden
  - **Ubuntu/Debian:** das Paket `pidgin-otr` installieren

# Weitere Infos

**<https://hickerspace.org/crypto>**

Falls es Komplikationen gibt, kommt Freitags ab 20.00 Uhr vorbei.