Verschlüsselung mit OpenPGP

Sichere Email Kommunikation für Alle

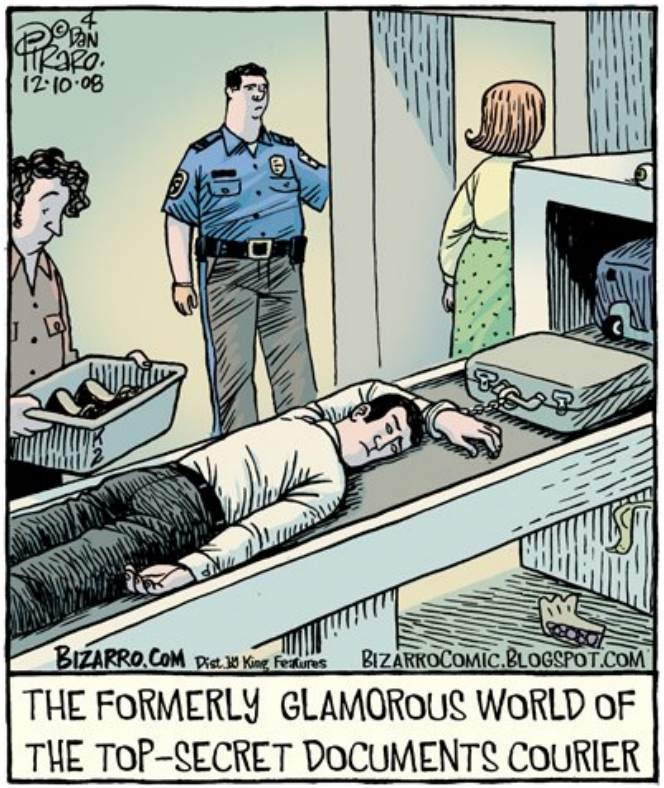
Linus Lüssing

Cryptoparty, 24. Jan. 2015, Chaotikum e.V. / Lübeck

Outline

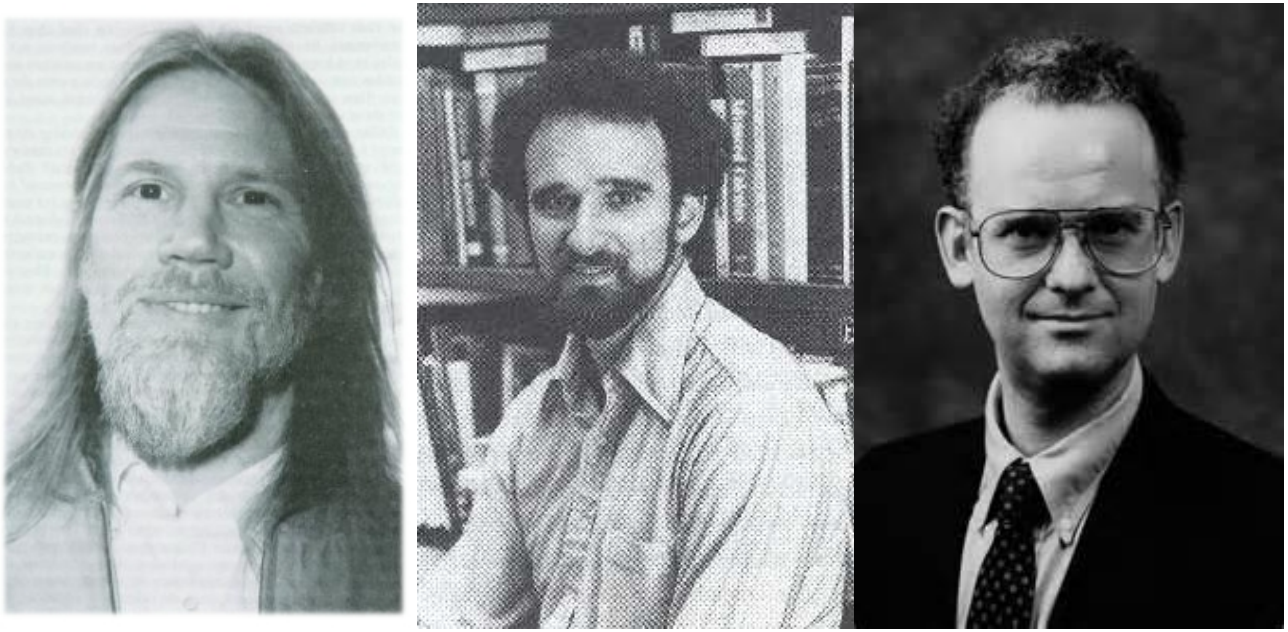
1. Asymmetrische Verschlüsselung
2. Pretty Good Privacy

Nachteil Symmetrischer Verschlüsselung



- Vor asymmetrischen Verschlüsselung:
  Schlüsselaustausch aufwendig

Öffentlicher + Privater Schlüssel



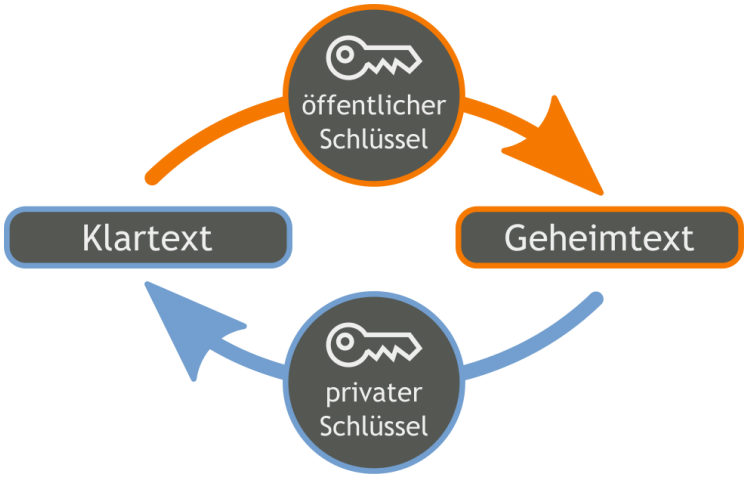
- Whitfield Diffie, Martin Hellman, Ralph Merkle
- Erfinder der asymmetrischen Verschlüsselung (1975)
- Aber war weiterhin gesucht: Einwegfunktion mit "Hintertür"

[Schlösser-Analogie]

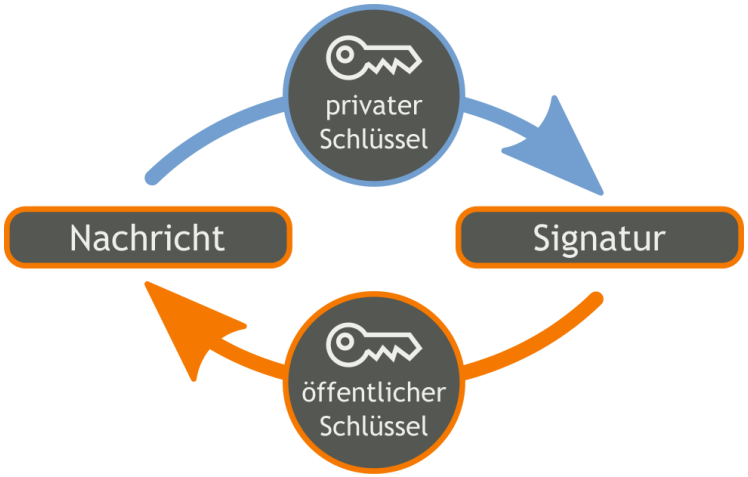
RSA-Verfahren (1977)

- Ronald L. Rivest, Adi Shamir und Leonard M. Adleman
- Einwegfunktion: Primzahlmultiplikation (/Primfaktorzerlegung)
- Einfach: $3079 \times 9967 = 30688393$
- Schwer: $53547797 = ? \times ?$

Verschlüsseln vs. Signieren



Ver- und Entschlüsselung



Signieren und Signaturprüfung

Bildquelle: Wikipedia, Lizenz: CC-BY-SA

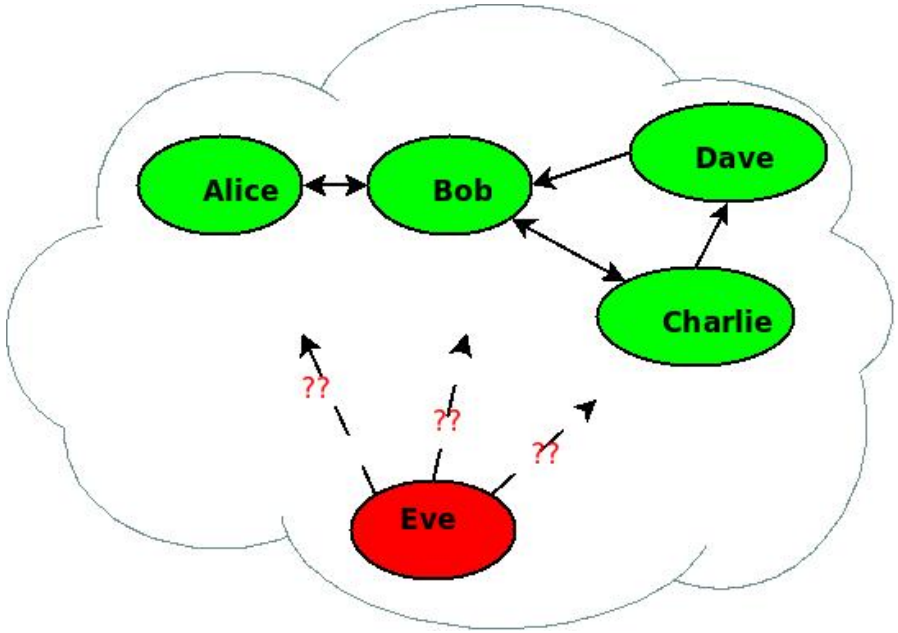
- Verschlüsselte Nachricht erhalten - aber von wem?
- *Verschlüsseln & Signaturprüfung:* Öffentlichen Schlüssel
- *Entschlüsseln & Signieren:* Privater Schlüssel

Pretty Good Privacy (1991)

Bildquelle: Wikipedia, Lizenz: CC-BY-SA

- Computerprogramm von Phil Zimmermann
- Sichere Verschlüsselung für alle
- Internet-Standard: OpenPGP

Web of Trust



- Durchschnittliche Distanz zwischen zwei Menschen: ~6
- Idee: ”Verbürgen” für die Identität eines anderen
  $\Rightarrow$ Signieren von öffentlichen Schlüsseln
- Zum Durchforsten: *http://pgp.cs.uu.nl/*

Zusammenfassung

- Asymmetrische Verschlüsselung:
  $\Rightarrow$ Zwei statt ein Schlüssel
  - *Öffentlicher Schlüssel:* Verschlüsseln + Signaturprüfung
  - *Privater Schlüssel:* Entschlüsseln + Signieren
    Wichtig!!!: Geheim halten!
- Web of Trust: Sichere Kommunikation mit ”Dritten”
  Wichtig!!!: Nicht jeden Schlüssel signieren!

Responsible Behavior

https://xkcd.com/364/ (Lizenz: CC-BY-NC)

- Next: *Hands on!*