Einführung Kryptographie

Matthias Geiser

<matthias.geiser@siug.ch>

Swiss Internet User Group (SIUG)

Big Brother Awards Schweiz

Zwei Arten der Verschlüsselung

- symmetrische Verschlüsselung
- asymmetrische / public key Verschlüsselung

Symmetrische Verschlüsselung

- Ein Schlüssel: Wer den Schlüssel hat kann sowohl entschlüsseln wie auch verschlüsseln.
- Vergleich: Türschloss, Tresor
- Alt: über 3000 Jahre: Griechen, Spartaner, Caesar

Vorteile: schnell, relativ einfach

Nachteile: Keine Kontrolle über Schlüssel, braucht sichere Schlüsselverteilung

Public Key Verschlüsselung (1)

- Zwei Schlüssel: Ein Schlüssel zum Verschlüsseln, einer zum Entschlüsseln.
- Vergleich: Vorhängeschloss, Schnappschloss
- Neu: 1976 Diffie, Hellmann, 1977 Rivest, Shamir, Adelmann

Nachteile: langsam, basiert auf mathematischen Vermutungen

Vorteile: Public Key muss nicht geheimgehalten werden → Schlüsselaustausch ist einfach

Public Key Verschlüsselung (2)

Schlüsselverteilung: Schlüssel auf öffentlichem Schlüsselbrett (Telefonbuch)

Problem: Gehört der Schlüssel wirklich Alice?

Lösung: Schlüssel werden beglaubigt (Zertifikat)

Problem: Ist die Zertifizierungsstelle vertrauenswürdig?

- Staat?
- Wirtschaft?
- Freunde!

Email Verschlüsselung

- PGP (Pretty Good Privacy)
- 1991 Phil Zimmermann
- Gratis! → `http://www.pgpi.org`
- Sicher!
- Gute Einbindung in verbreitete Email-Programme

Literatur, Links

Einführung:

- A. Beutelspacher: Kryptologie
- `http://www.siug.ch/help/SIUG-Kryptoeinfuehrung`

Geschichte:

- S. Singh: The Code Book
- D. Kahn: The Codebreakers

PGP:

- `http://home.nexgo.de/kraven/pgp/pgpf.html`
- `http://www.pgpi.org`
- `http://gnupg.org`