Asymmetrische Verschlüsselung im Einsatz
Mailen mit GnuPG

Moritz Bubek

Übersicht

- Motivation
- Verschlüsselung
- Asymmetrische Verschlüssel & RSA
- PGP / GnuPG
- Web of Trust

Wieso eigentlich dieser Vortrag?

- Simon will GPIB Karte einrichten
- Moe muß helfen
- lange Prozedur
- Moe will Account
- Simon erstellt Account ...
- Simon will Daten verschicken, ABER


Bundesnachr
CENTRAL
ENCE AGENCY
UNITED STATES OF AMERICA


007
DIE ANOTHER DAY
11.22
JAMES BOND
www.mgm.com
www.jamesbond.com
© 2001-2002 METRO-GOLDWYN-MAYER STUDIOS INC. ALL RIGHTS RESERVED.
DIE ANOTHER DAY ™ TRADEMARK UNITED ARTISTS CORPORATION AND DANJAQ, LLC.
JAMES BOND MATERIALS © 1962-2002 UNITED ARTISTS CORPORATION AND DANJAQ, LLC.
007 GUN LOGO, JAMES BOND, AND ALL OTHER JAMES BOND RELATED TRADEMARKS ™ DANJAQ, LLC.

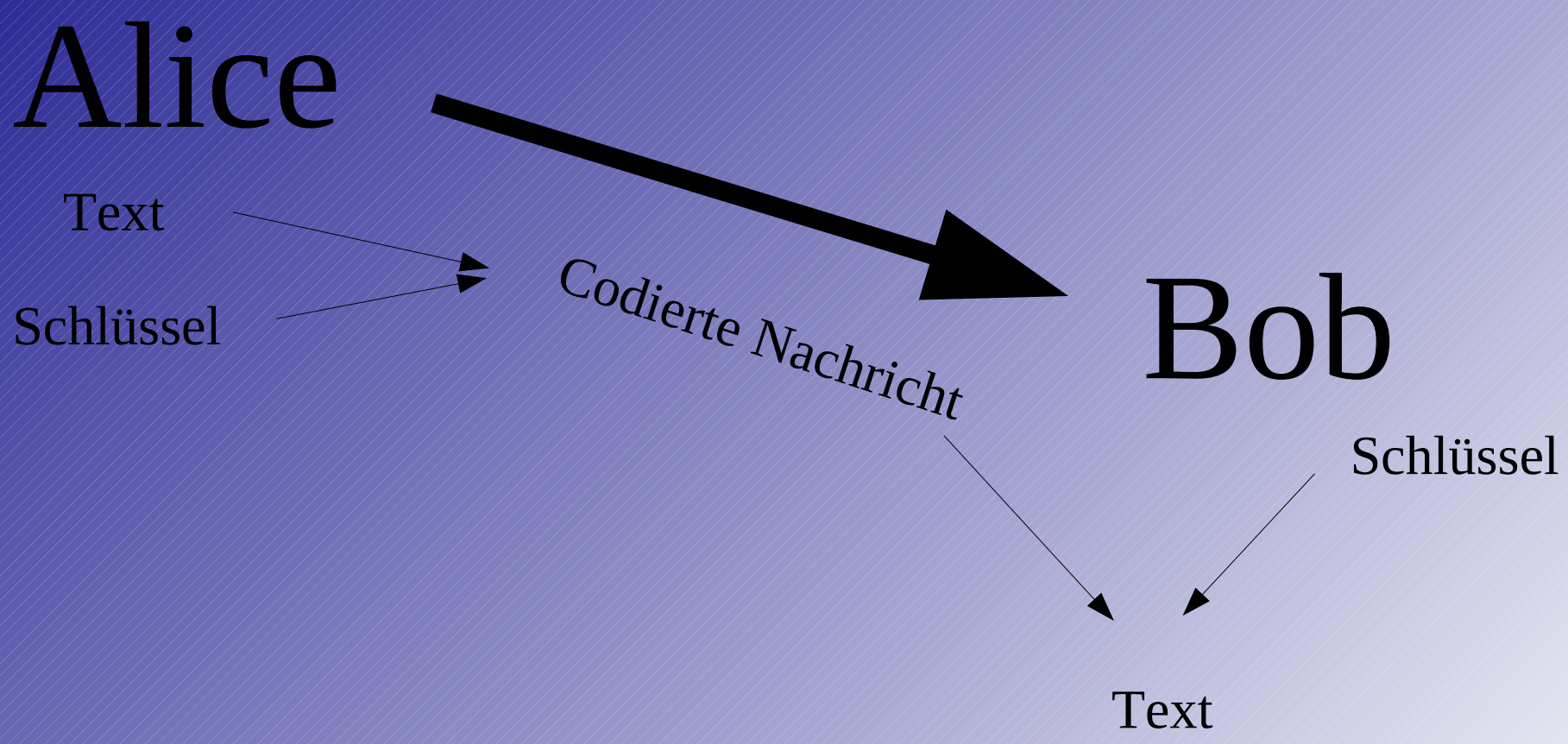
Wer und Warum

- Email weniger vertraulich wie eine Postkarte
- Administratoren der Mailserver, Mail wird gespeichert !
- Hacker und Cracker
- planmäßiges Eindringen durch Geheimdienste
- Wirtschaftspionage, Wissenschaftsspionage
- (Strafverfolgung)

Mittel dagegen: Verschlüsselung

- Kommunikation verschlüsseln
- uralte Idee (Babylon, Griechen, Römer, ...)
- zuerst einfaches Ersetzen von Buchstaben (rot13)
- durch Statistik leicht zu knacken
- Verbesserung: Verschlüsselung mit Schlüssel (IDEA, Blowfish, ...)
- Text XOR Key
- nur OTP wirklich sicher !

Grundprinzip



Und wieso tuts nicht ?

- Problem 1: Schlüssel muß übertragen werden
  Unsicherer Kanal
  Eve fängt Schlüssel ab, alles umsonst
- Problem 2: ist mein Partner der für den er sich ausgibt?
  Authentifizierung
- Problem 3: n (n-1)/2 viele Schlüssel nötig !

asymmetrische Verschlüsselung

- Schlüsselpaar aus zwei Teilen
- öffentlicher Schlüssel - public key
- geheimer Schlüssel - private key
- mit publicKey verschlüsseln, mit privateKey entschlüsseln
- Falltür-Algorithmus

am Beispiel RSA

- Wahl zweier Primzahlen p und q (500 Stellen)
- Produkt $N = p*q$ berechnen
- Eulersche Funktion $\Phi(N) = (p-1)(q-1)$
- Wähle e mit $1 < e < \Phi$ teilerfremd
- berechne d, sodass $e*d \bmod \Phi = 1$
- publicKey: e, N ; privateKey: d, N
- Rest löschen !

Anwenden von RSA

- Verschlüsseln

$$C = K^e \bmod N$$

- Entschlüsseln

$$K = C^e \bmod N$$

Sicherheit von RSA

- kennt Eve Φ kann d leicht berechnet werden
- nur mit N --> Primfaktorzerlegung
- Schlüssellänge schlecht vergelichbar, heute 1024 Bit sicher

Anwendungsfall: PGP / GPG

- PGP: Zimmermann 1991
- Opensource Variante wegen Patenten
- Schlüssel auf Schlüsselservern
- gpg –gen-key
- Name und Emailadresse, dazu ein Mantra
- wichtig: am besten sofort Widerruf erzeugen (gpg –gen-revoke keyID)

Exportieren/Importieren

- gpg –export bubek@gmx.de
- gpg –search thomay
- Signieren von Schlüsseln
  gpg --edit-key
  sign
- Editieren, Widerrufen, ...

Verschlüsseln/Entschlüsseln

- gpg –encrypt –recipient sverleger@gmx.de
- gpg –decrypt datei
- im Mailprogramm direkt mit drin (Plugin?!)

Komfortabler?

GNU Privacy Assistant - Schlüsselverwaltung

Datei Bearbeiten Schlüssel Server Fenster Hilfe

Schlüsselverwaltung

Schlüsselkennung	Benutzerkennung
D79D9769	Moritz Bubek <bubek@gmx.de>
62DC155E	Simon Verleger <simon.verleger@uni-konstanz.de>
7B06C9A1	Simon Verleger (GMX) <sverleger@gmx.de>
67E78738	Stefan Boehrer <Stefan.Boehrer@gmx.de>
9B42CF5A	Michael Hanfland <mh@tomix.de>
8B14831D	Niels Ott (Standardschlüssel 1) <niels@drni.de>
ED7CF01D	David Feise (privat) <david@feise-de.de>
91848AC1	Amarendran R. Subramanian <amar@neckar-alb.de>

Details | Signaturen | Untergeordnete Schlüssel

Keine Schlüssel ausgewählt

Standard-Schlüssel: Moritz Bubek <bubek@gmx.de> D79D9769

test 17766

Sicherheit

- Mit PGP signieren
- Mit PGP verschlüsseln
- Mit S/MIME signieren
- Mit S/MIME verschlüsseln

Einfügen Suchen Ersetzen

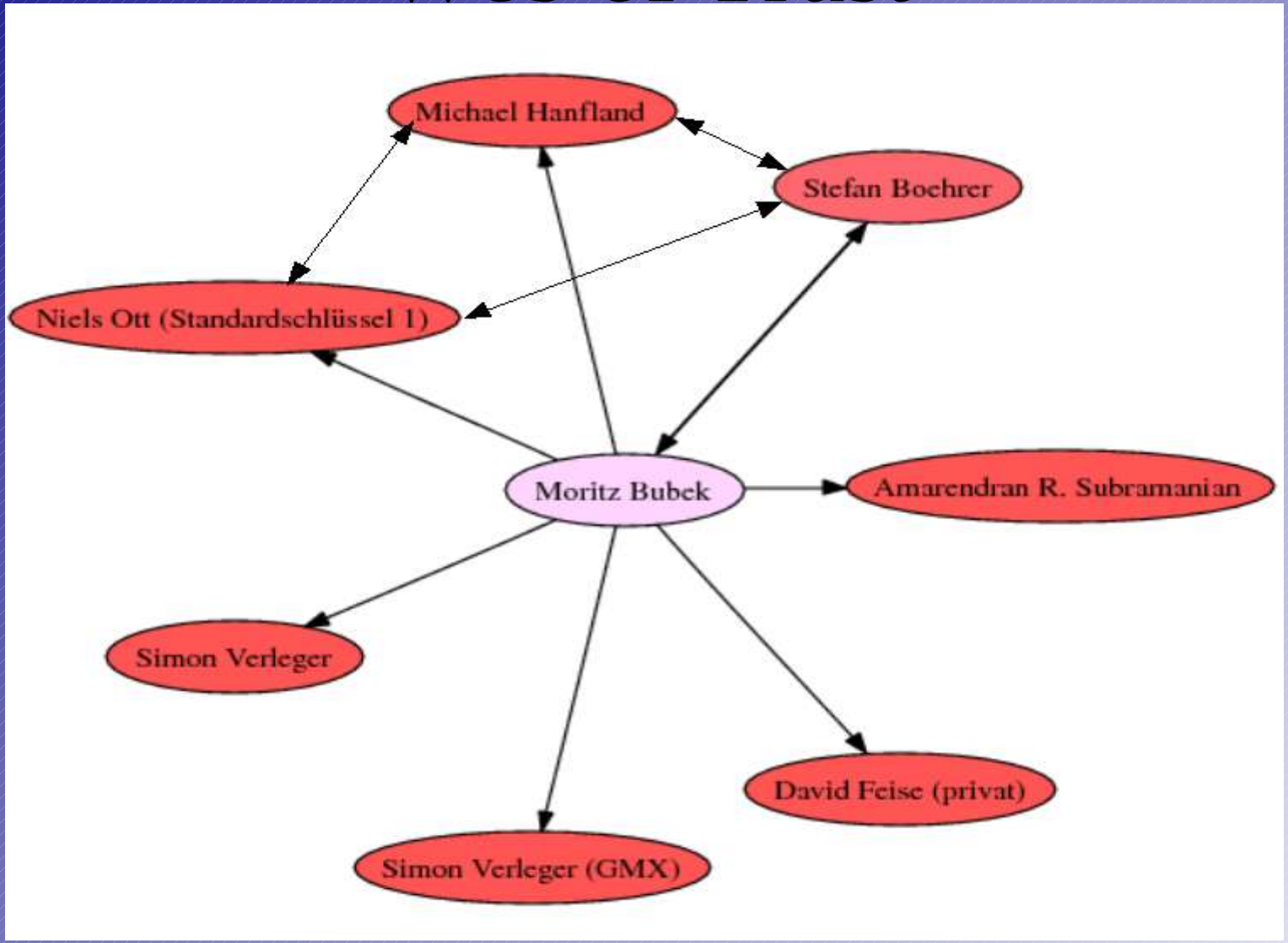
Signatur: Keine

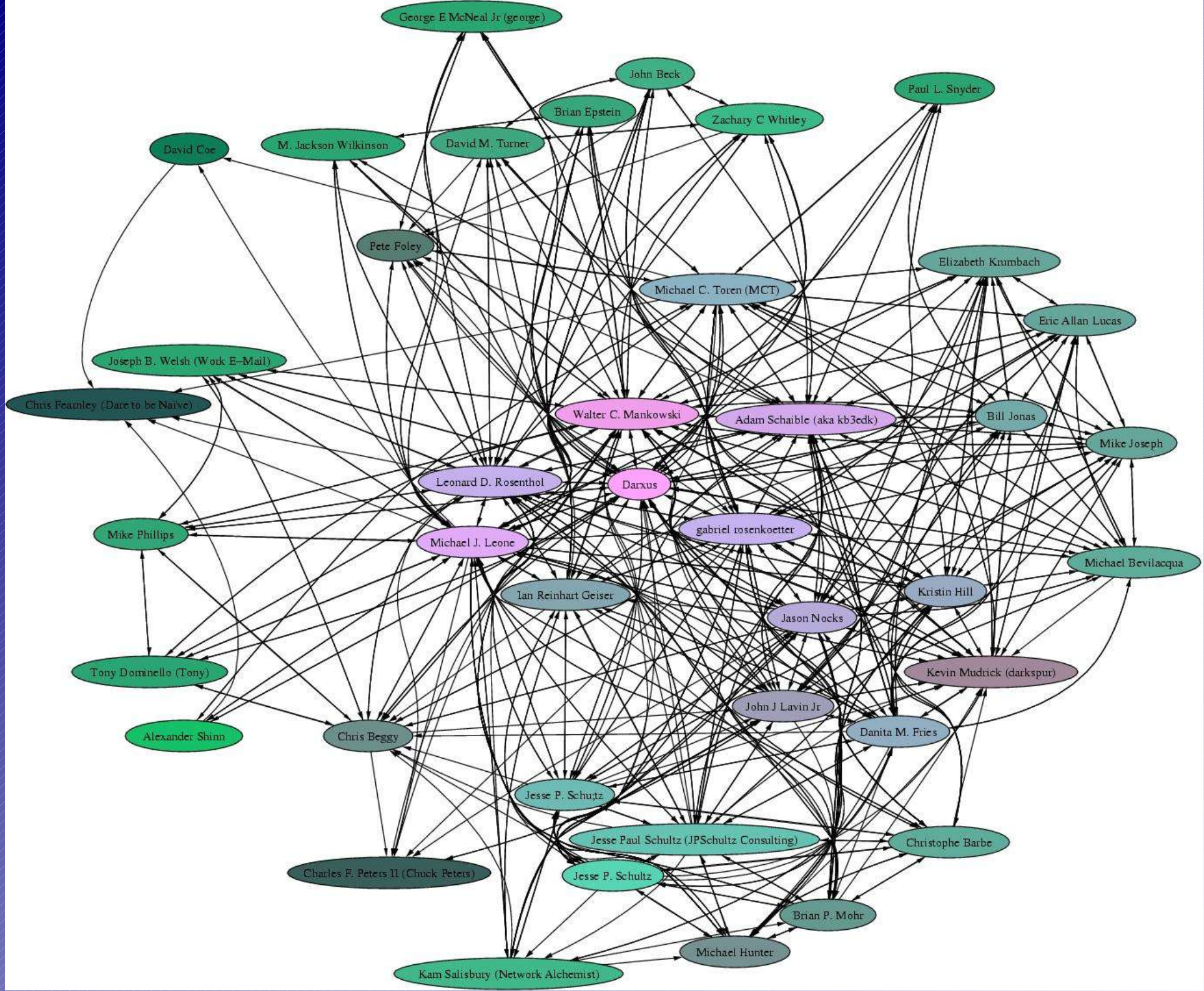
Anlagenleiste anzeigen (legen Sie Anlagen hier ab)

Mit wem rede ich eigentlich?

- Problem: Authentifzierung
- Lösung: Signatur mit privateKey verschlüsseln (umgekehrt !)
- Empfänger kann mit publicKey Entschlüsseln
- bei Übereinstimmung alles ok

Web of Trust


Michael Hanfland
Stefan Boehrer
Niels Ott (Standardschlüssel 1)
Moritz Bubek
Amarendran R. Subramanian
Simon Verleger
David Feise (privat)
Simon Verleger (GMX)


George E McNeal Jr (george)
John Beck
Paul L. Snyder
Brian Epstein
Zachary C Whitley
David Coe
M. Jackson Wilkinson
David M. Turner
Pete Foley
Elizabeth Krumbach
Michael C. Toren (MCT)
Eric Allan Lucas
Joseph B. Welsh (Work E-Mail)
Chris Fearnley (Dare to be Naive)
Walter C. Mankowski
Adam Schaible (aka kb3edk)
Bill Jonas
Mike Joseph
Leonard D. Rosenthol
Darxus
Mike Phillips
gabriel rosenkoetter
Michael J. Leone
Michael Bevilacqua
Ian Reinhart Geiser
Kristin Hill
Jason Nocks
Tony Dominello (Tony)
Kevin Mudrick (darkspur)
John J Lavin Jr
Alexander Shinn
Chris Beggy
Danita M. Fries
Jesse P. Schultz
Jesse Paul Schultz (JPSchultz Consulting)
Christophe Barbe
Charles F. Peters II (Chuck Peters)
Jesse P. Schultz
Brian P. Mohr
Michael Hunter
Kam Salisbury (Network Alchemist)

Fazit

- Möglichkeit vorhanden
- trotzdem kaum benutzt
- erstellt euch ein Schlüsselpaar
- KeySigning Party

Quellen

- www.gnupg.org
- de.wikipedia.de
- www.lysator.liu.se/~ceder/
- www.chaosreigns.com
- myself