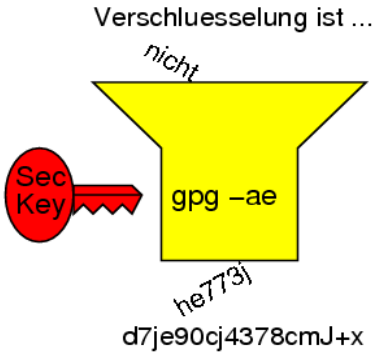
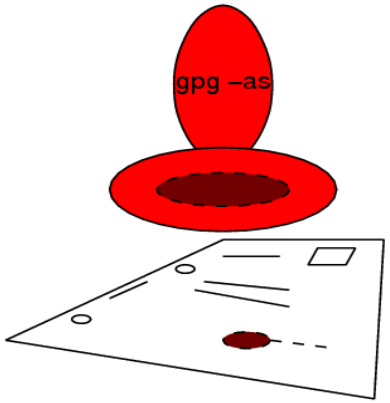
Verschlüsselung und elektronische Signaturen

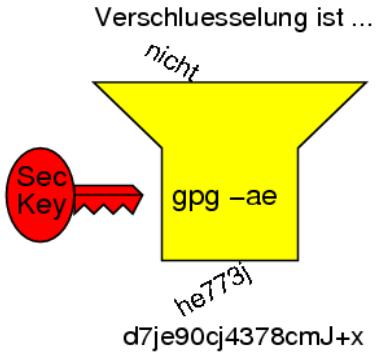
Joerg.Schulenburg_at_ovgu.de





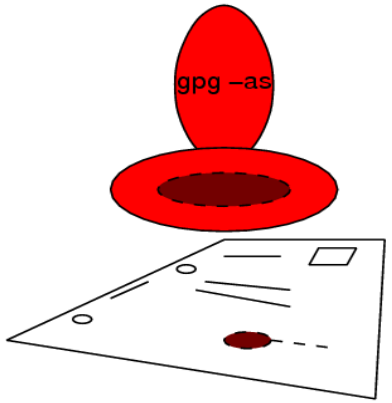
Was ist Verschlüsselung? (kurz)

- Umwandlung von Klartext in Geheimtext
- mit dem Ziel, Klartext vor Unbefugten  zu verbergen



Was ist eine elektronische Signatur? (kurz)

- (elektronischer) Ersatz für handgeschriebene Unterschrift (jurist.)
- lt. Wikipedia verschieden von “digitaler Signatur” (meinte ich wohl)
- digitales Anhängsel zur Prüfung von Urheberschaft und Zugehörigkeit



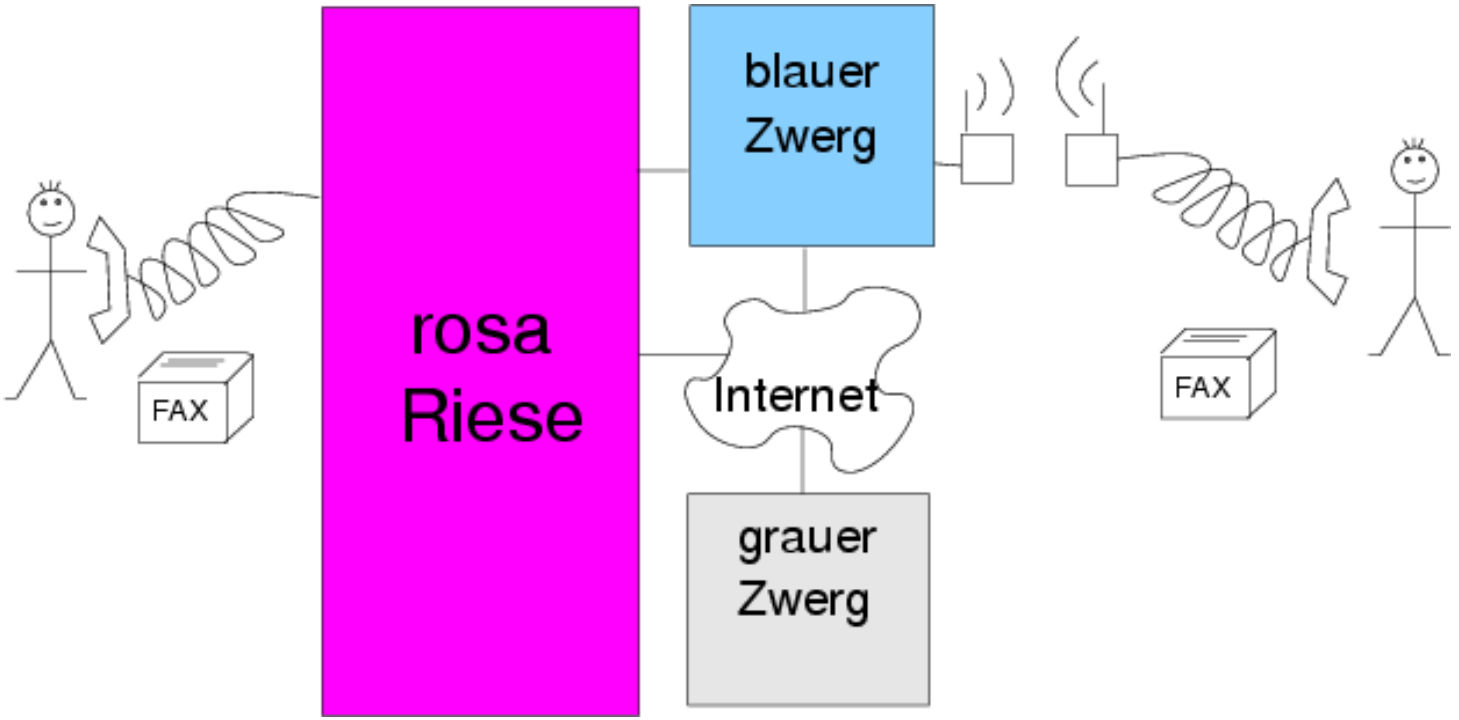
Wozu brauchen wir das?

Ist doch alles sicher!

Zu einfa

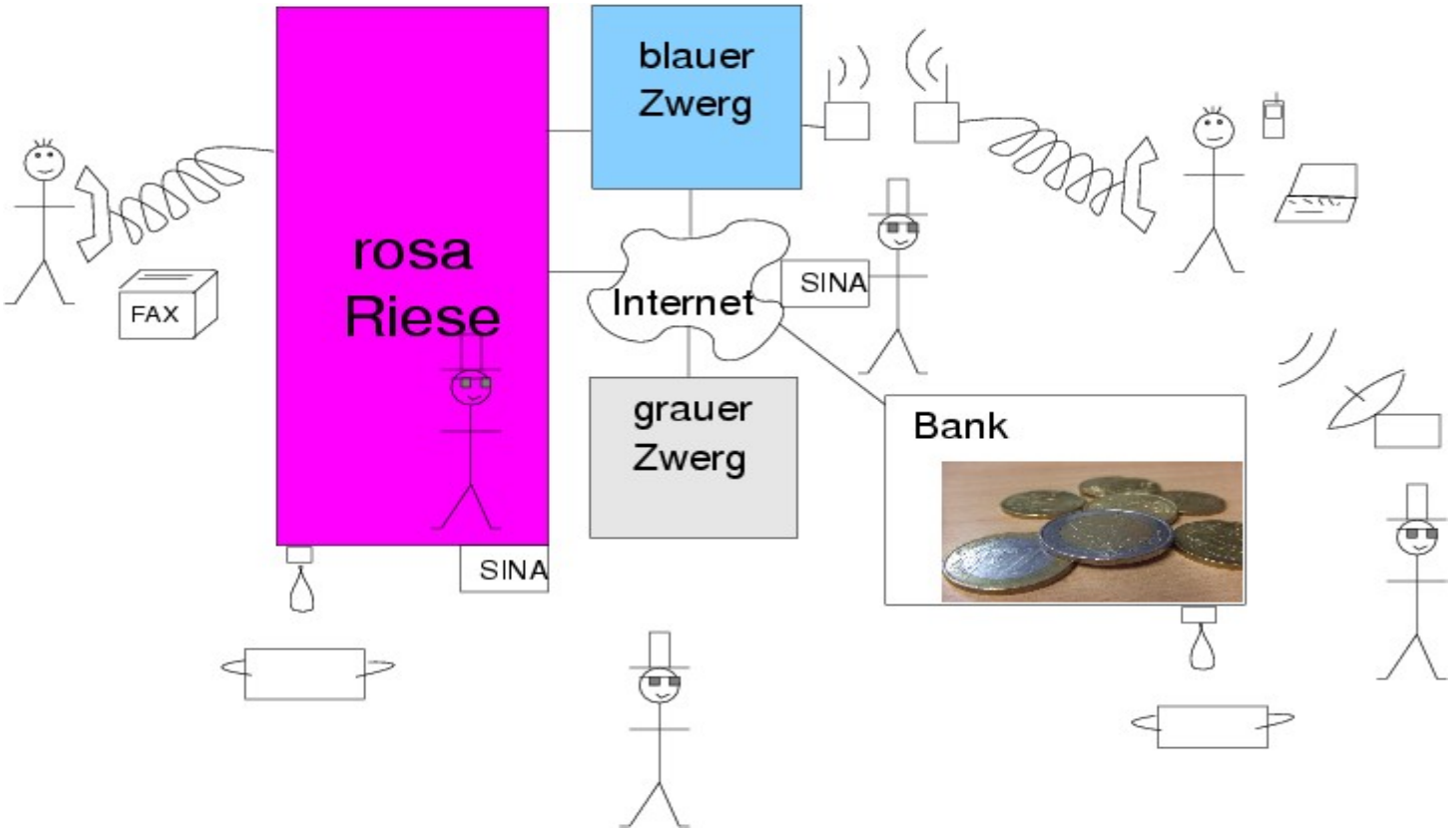
Wozu brauchen wir das?

... realistischer



Wozu brauchen wir das?

… unüberschaubare Zahl von Mißbrauchsrisiken



Wozu brauchen wir  das? (theoretisch)

- sichern gegen mitlauschen durch Dritte
- sichern gegen Verfälschung
- Verläßliche (Absender-)Identifizierung

Wozu brauchen wir  das? (praktisch)

- (autom.) download von digital signierten Programmpaketen
- bequeme Geld- und andere Geschäfte via Internet
- vertrauliche EMAILs (Uni: Verwaltungsdaten)
- Schutz bei Verlust der Hardware und mögl. Mißbrauch
- ...
- $(Ergänzungen von Euch ?)

Was hindert uns, GnuPG und co. zu nutzen?

- erhöhter Strom und Zeitverbrauch? (wohl kaum)
- Bequemlichkeit

Komplexität (wirklich?)

Nulltarif?

Leidensdruck + Mißtrauen (wächst)

- Mitmachen des Kommunikationspartners

Ist Verschlüsselung etc. komplex?

- wenn man es richtig machen will, schon
- SSL im Webbrowser als Beispiel
  - schlechte Keys made by Debian systems (2008)
  - rückgerufene Zertifikate (woher?)
  - selbstsignierte Zertifikate (Warnung des Browsers) = schlecht?
  - DFN und Mozilla Foundation, versus Default RootCAs = gut?
  - Cross-Site-Attacks, Flash, Javascript
- Aber Wissen um Verschlüsselung und Co. bringt wie so oft Vorteile

Partner für GnuPG etc.?

- Banken (Idealanwender) sind lernresistent
  - SSL/RootCA Prüfsummen nur im Browser?
  - fordern Javascript für Webseiten, EMAILen im Klartext
  - signierte digitale Bankauszüge (wer kennts?)
- Telekom und Konsorten
  - Rechnungen per EMAIL (klartext) aufgedrängelt, (pos. Bsp?)
  - digital signiert? (positive Beispiele? = StratoDSL, ...)
- Compute-Server (ssh statt telnet durchgesetzt)
- ...
- Wir müssen mehr Druck machen!

Wie funktioniert (theor.) Verschlüsselung?

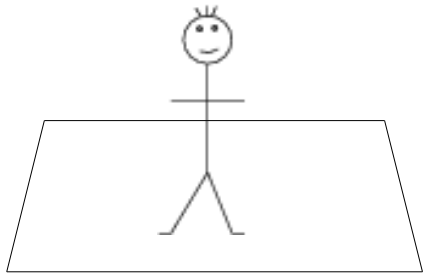
- symmetrisch (Blowfish, IDEA):
  - schnell
  - shared secret (paarweise, skaliert nicht)

- asymmetrisch:
  - langsam
  - „public key“ = Produkt zweier Primzahlen, wird veröffentlicht (unfälschbar!)
  - „secret key“ = Primzahlpaar, muß geheim bleiben (zusätzl. Passphrase, .gnupg/secring.gpg)

- one-time-pad (TANs) + Quantenkryptographie(macht OTP praktischer, aber Skalierung(-))

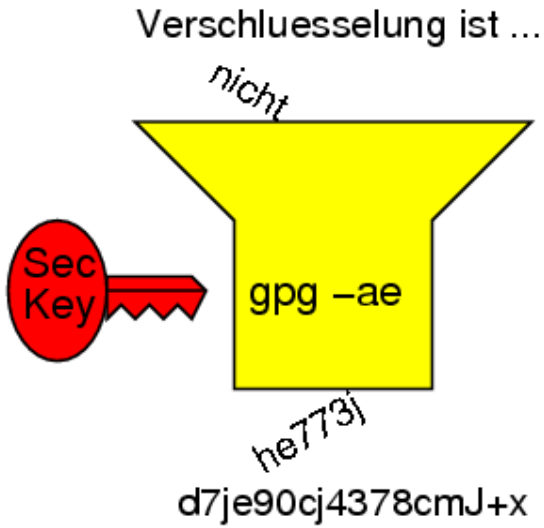
Wie funktioniert (theor.) Verschlüsselung?

- Falltürfunktionen (asymmetrisch):
  - Primzahlprodukte
  - hineinfallen (privat key): 41*19=?
  - ... und wieder hinauskommen (public key): 713=?*?



Wie funktioniert prakt. Verschlüsselung?

- symmetrischen Key generieren und mit Public-Key verschlüsseln
- komprimierung des Klartextes
  (z.B.: tar -c path | gnupg -c path.tar.gpg reicht, implizit gzip)
- symmetrisches verschlüsseln des Komprimates

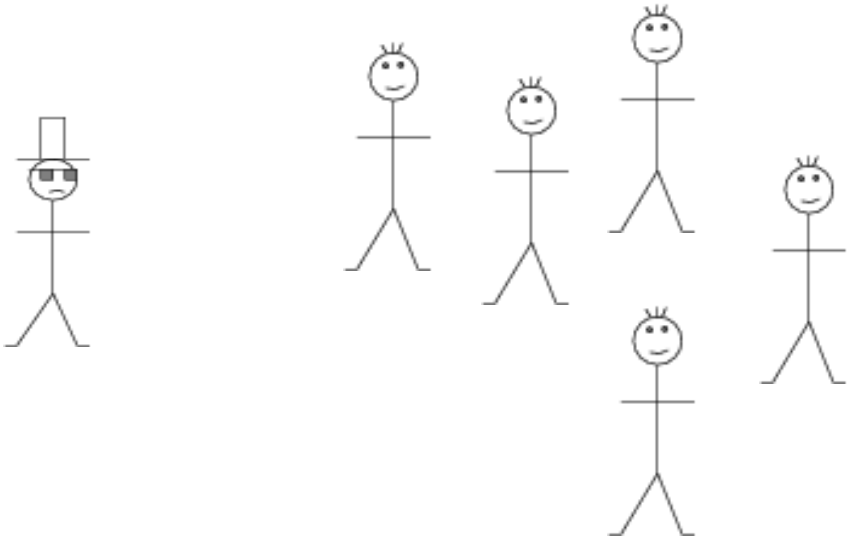


Wie funktioniert prakt. Verschlüsselung?

...

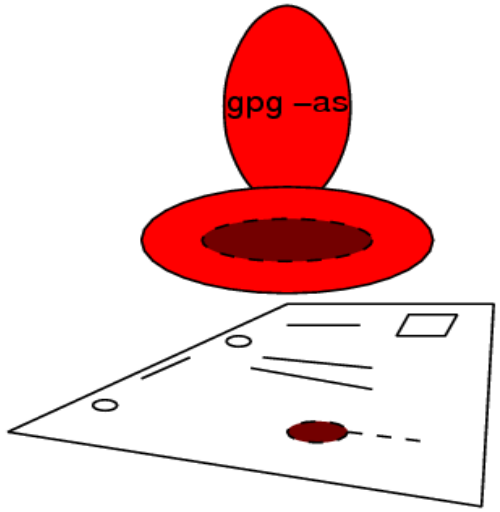
+ Web of trust (PGP Keyserver, .gnupg/pubring.gpg + trustring.gpg)

- Fälschung muss unmöglich sein



Wie funktioniert die digitale Signatur?

- Hash aus Klartext generieren (MD5, SHA1)
- Hash mit Secret-Key verschlüsseln



Schwachstellen?

- grundsätzlich fehlender mathematischer Beweis der Sicherheit
- Hash-Kollisionen (Paargenerierungen, Zufallserweiterungen etc.)
- kurze oder schwache Schlüssel (versus Rechen-/Speicheraufwand, schlechte Zufallszahlen)
- gefälschte Public-Keys (mangelnde Prüfung, mangelhafte Öffentlichkeit)
- Geheimhaltung des Secret-Keys (Viren, Trojaner, Backdoors, NFS)
- mangelhafte Implemetierungen (schlechte Zufallsgeneratoren, ...)
- ...

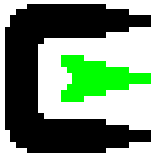
OK, legen wir los!

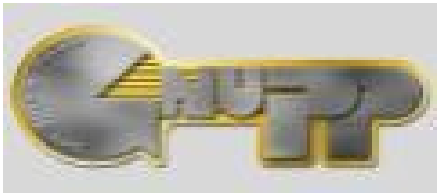
Welche Programme?

- no Closed Source! (Hintertüren, Generalschlüssel, Fehler)
- OpenSource? (Ja! Nur! OSS = Transparenz = Vertrauen)
  - PGP? (das Original? Patente!)
  - GnuPG? (ja, bewährtes Jedermannsprogramm = verbreitet)
  - OpenSSL, S/MIME? (ja, aber hierarchische Zertifikatsstruktur)
  - GnuPG + OpenSSL Library basierende ...
  - und wenns nötig ist, grafische Oberflächen dazu :)
  - ...

Welche Programme?

- www.GnuPG.org
- Linux: gnupg meist enthalten, GPA
- Windows: Cygwin, GnuPP (GnuPG+GPA+WinPT)





Welche Programme?

- gnupg (CLI Version, universell)
  - Schlüsselpaar generieren (--gen-key, --list-keys)
  - Public-Key importieren/exportieren (--import, --export -a)
    prüfen (--fingerprint)
    keyserver (--search-keys, --send-keys
    --keyserver hkp://www.keyserver.net)
  - Signatur erzeugen/prüfen (-a --sign, --verify)
  - Datei verschlüsseln/entschlüsseln (-ae, -d)

Und nun …?

… ausprobieren und verbreiten!

Quellen:

- www.wikipedia.de (Verschlüsselung, GnuPG, PGP, ...)
- J.M. Ashley, GNU Privacy Handbuch (GPH als PDF-Datei)
- T. Bader, Geheimsache, Linux-Magazin 12/1999
- Christian Kirsch, Mailchiffrierung mit GnuPG, iX-Magazin 3/2004
- www.dfn-pca.de
- www.sicherheit-im-internet.de

Danke!