eMail-Verschlüsselung für Einsteiger

Kai 'zeus' Kostian ⟨zeus@ctdo.de⟩

Chaostreff Dortmund

Lightning Talks beim Ping e.V.
14.11.2015

Index

Was ist Verschlüsselung?

Verschlüsselung (auch: Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.[1]

- Die Anfänge: Caesar-Verschlüsselung
- Durchbrüche der Verschlüsselung: Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und asymmetrische Schlüsselverfahren

[1] Quelle: `https://de.wikipedia.org/wiki/Verschl%C3%BCsselung`

Was ist Verschlüsselung?

Verschlüsselung (auch: Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.[1]

- Die Anfänge: Caesar-Verschlüsselung
- Durchbrüche der Verschlüsselung: Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und asymmetrische Schlüsselverfahren

[1] Quelle: `https://de.wikipedia.org/wiki/Verschl%C3%BCsselung`

Was ist Verschlüsselung?

Verschlüsselung (auch: Chiffrierung) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.[1]

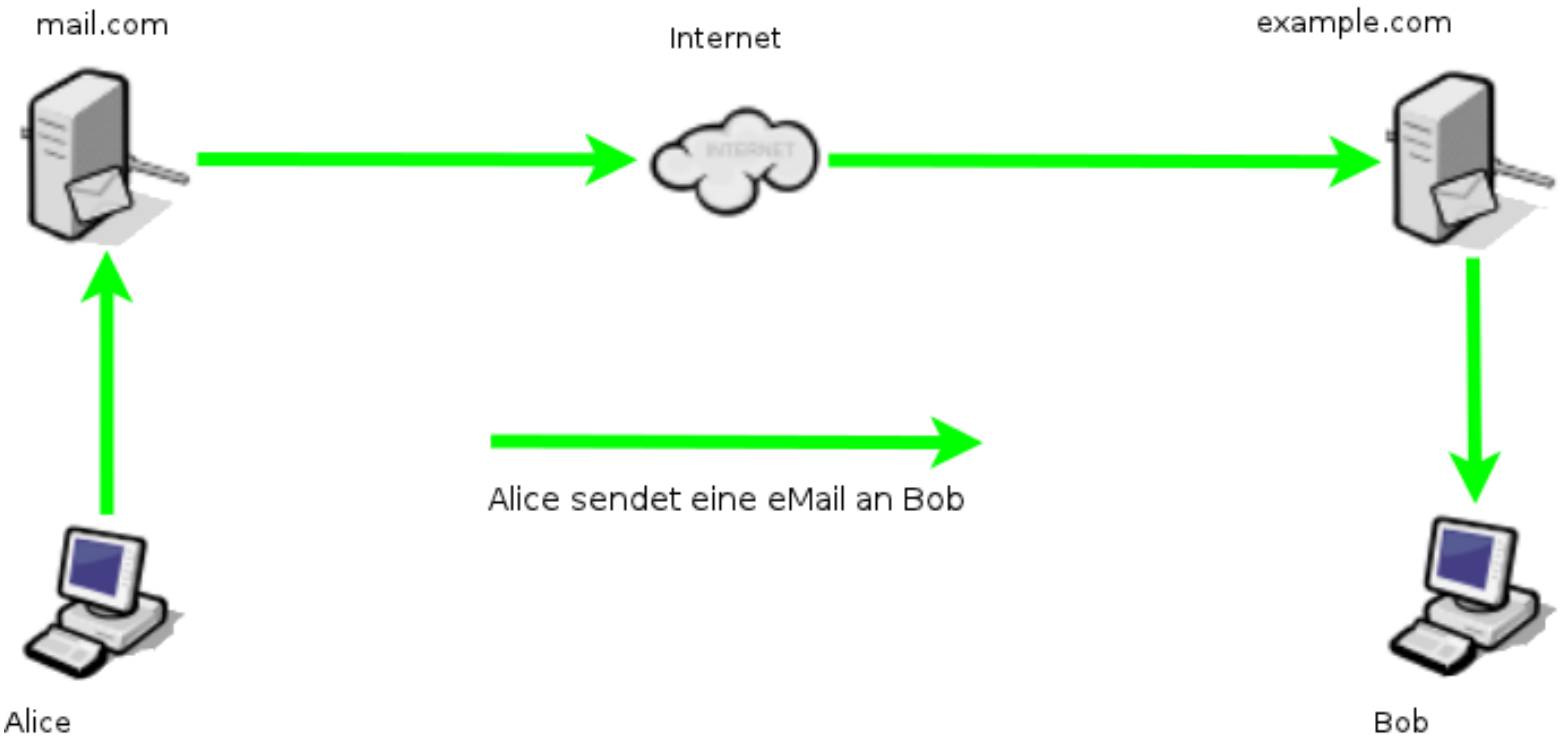
- Die Anfänge: Caesar-Verschlüsselung
- Durchbrüche der Verschlüsselung: Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und asymmetrische Schlüsselverfahren

[1] Quelle: `https://de.wikipedia.org/wiki/Verschl%C3%BCsselung`

eMail-Grundlagen

- Elektronische Post seit 1984
- Mails bestehen aus einem Header (Metadaten) und dem Body (Nachrichten, Anhänge)
  $\Rightarrow$ Wichtig: Der Betreff gehört zum Envelope (Header!)
- Verschlüsselte Kommunikation nur bis zum eigenen Provider ohne Zusatzsoftware möglich (Transportverschlüsselung)
- eMails passieren im "Klartext" meist einige bis einige dutzend Server

eMail mit Alice und Bob



Der Bedarf an Vertraulichkeit

- Je **peinlicher**, **persönlicher** oder **brisanter** eine Information ist, desto mehr Bedarf an Vertraulichkeit ist vorhanden
- Je **teurer** es ist, wenn Informationen in die falschen Hände gelangen, desto mehr Bedarf an Vertraulichkeit ist vorhanden

⇒ Fazit: Alles verschlüsseln, was verschlüsselbar ist

Der Bedarf an Vertraulichkeit

- Je **peinlicher**, **persönlicher** oder **brisanter** eine Information ist, desto mehr Bedarf an Vertraulichkeit ist vorhanden
- Je **teurer** es ist, wenn Informationen in die falschen Hände gelangen, desto mehr Bedarf an Vertraulichkeit ist vorhanden

$\Rightarrow$ Fazit: Alles verschlüsseln, was verschlüsselbar ist

Unterschied zwischen Transport- und Inhaltsverschlüsselung

Transport-Verschlüsselung $\neq$ Inhalts-Verschlüsselung!

- Transportverschlüsselung schafft eine sichere, **verschlüsselte** Verbindung, durch welche die Inhalte für Sender und Empfänger trotzdem im Klartext verfügbar sind.
- Transportverschlüsselung schützt nur vor Dritten, die von aussen auf die Verbindung sehen
- Inhaltserschlüsselung schützt vor Manipulation, vor Mitlesern und ermöglicht Authentifizierung des Kommunikationspartners
- Beides sind **ERGÄNZENDE** Verfahren
  - SSL/TLS (https,imaps, ..) $\rightarrow$ **Transport**verschlüsselungen
  - GPG, PGP u.Ä. sind Verfahren für **Inhalts**verschlüsselung

GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern (optional) und Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der **Authentizität** von Schlüsseln durch Fingerprints
- Überprüfbarkeit der **Integrität** von Nachrichten auf Manipulation
- Erweiterung von "Vertrauen" durch Keysigning (Chain of Trust / des Web of Trust)

GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern (optional) und Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

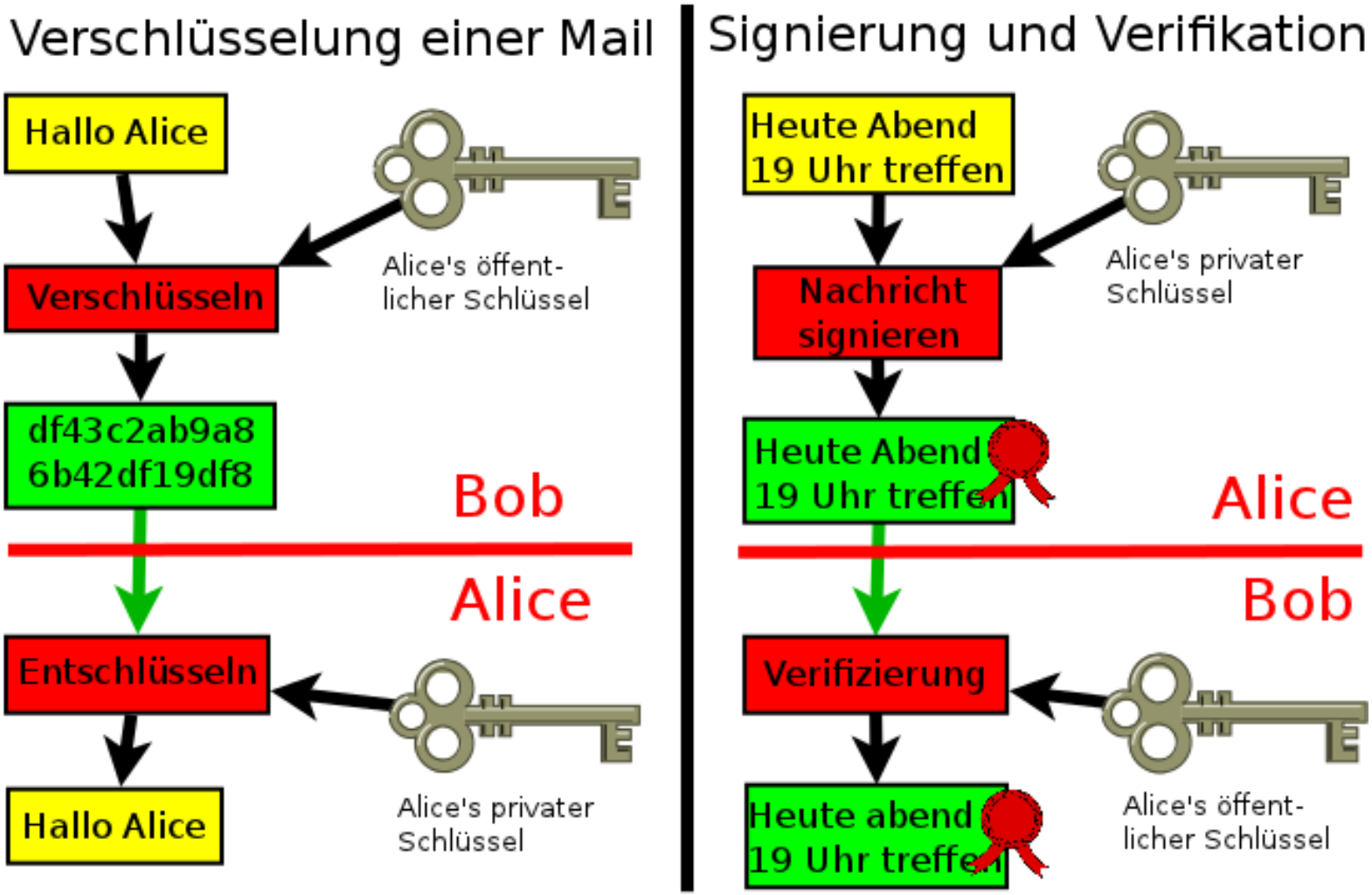
Vorteile:

- Überprüfbarkeit der **Authentizität** von Schlüsseln durch Fingerprints
- Überprüfbarkeit der **Integrität** von Nachrichten auf Manipulation
- Erweiterung von "Vertrauen" durch Keysigning (Chain of Trust / des Web of Trust)

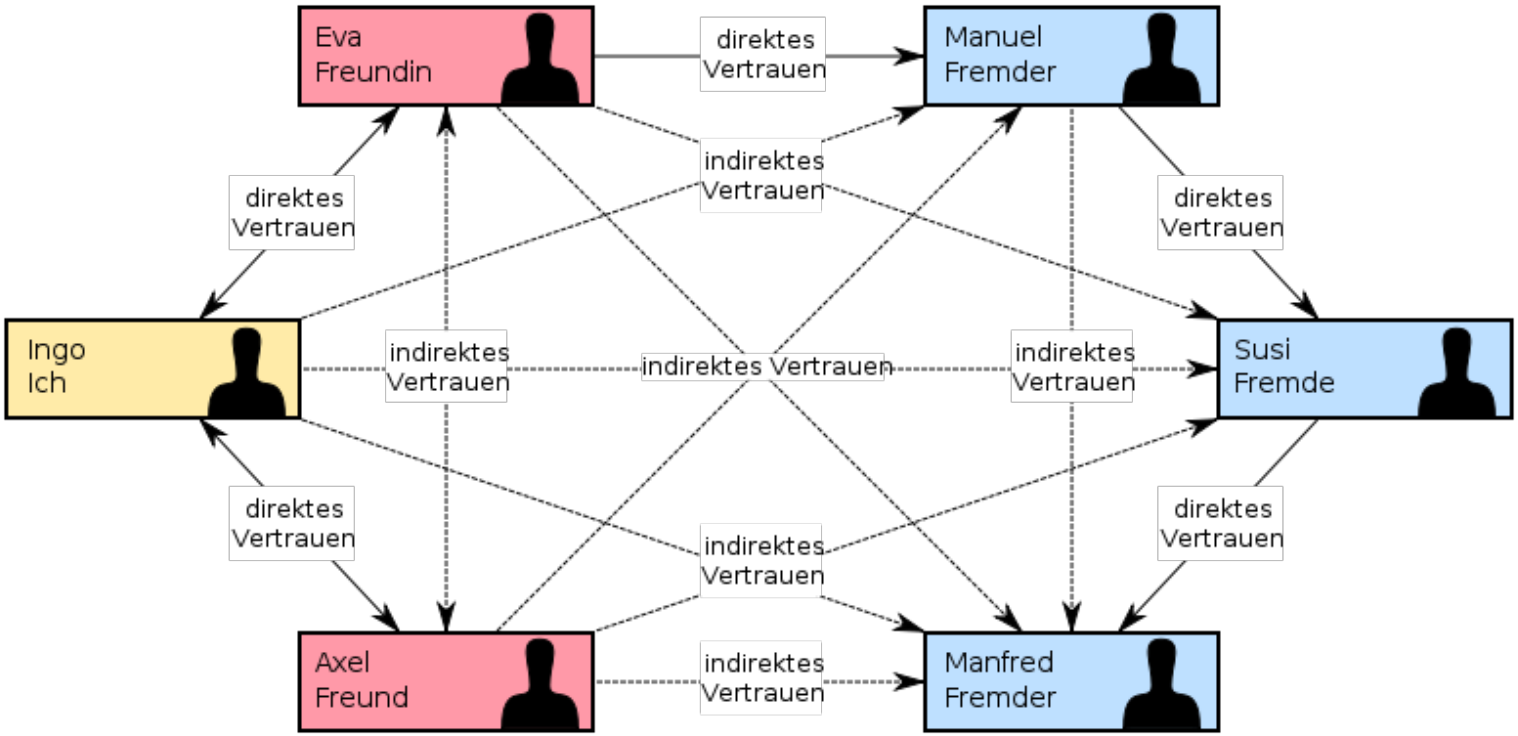
Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 4096 bit) und sicherem Passwort
  - **2 Schlüssel** werden erzeugt; **1 privater** und **1 öffentlicher**
  - Der **öffentliche Schlüssel** muss an alle künftigen Kommunikationspartner weitergegeben werden
  - Der **private Schlüssel** sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten **persönlich** vornehmen
  - Praktische Alternative für den Schlüsseltausch: **Keyserver**
  - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
  - $\Rightarrow$ Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger noch wichtiger als ohnehin schon !!

eMail-Verschlüsselung mit Alice und Bob



Web of Trust - Vertrauensketten



[2]

- Vertrauensketten durch direktes und indirektes Vertrauen
- Kurz: Ich vertraue Jedem, dem von Jemandem vertraut wird, dem ich vertraue

[2] http://de.wikipedia.org/wiki/Datei:Web_of_Trust.svg

Konzeptsicherheit: Die Theorie

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit ≥ 20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann

Konzeptsicherheit: Die Praxis

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetztung
- ...ist der Mensch der "Single Point of Failure" in diesem Modell
- ...passieren die meisten GAUs immernoch durch:
  - Dummheit
  - Naivität
  - Faulheit
  - oder (vor allem!) Schusseligkeit
- Das ist nun mal die Realität...

Backups

Do more Backups!

- Der goldene Weg: Auf Papier und/oder USB-Stick im Schliessfach/Tresor lagern, am besten redundant
  - Problem: bei Verlust/Verlegen des Keys ist das abtippen mühselig
- Fazit: Jedes Konzept hat seine Schwächen

Fancy Hardware

Es gibt da Hardware, womit das Ganze auch noch sicherer wird

[3]

[4]

- Links: Chipkarte ISO/IEC 7816
- Rechts: USB-CCID (chip card interface device)

[3] https://en.wikipedia.org/wiki/File:OpenPGP_card_2.0.jpg
[4] https://en.wikipedia.org/wiki/File:YubiKey_Neo_and_Nano.jpg

Smart Cards - Eigenschaften

- Prozessorkarte
- Unterschiedliche Anwendungen (Applets)
- Schlüssel in der Karte gespeichert
- Grundprinzip: Schlüssel kann die Karte nicht verlassen
- Prozessor der Karte führt Schlüsseloperationen durch
- Klonen der Karte oder kopieren der Schlüssel unmöglich

OpenPGP Card

- Offener Standard für PGP-Verschlüsselung mittels Smart Cards
- Dedizierte OpenPGP-Karten oder OpenPGP-Funktion in anderen Karten
- Platz für drei Schlüssel: Sign, Encrypt, Authenticate
- Schutz durch PIN / Admin-PIN: Sperre nach 3 Versuchen
- Funktionen zur Verwaltung / Nutzung in GnuPG integriert

OpenPGP Card in der Praxis

- gpg-agent: Nutzung von GnuPG wie gewohnt
- Karte muss eingesteckt sein, Eingabe von PIN anstatt Passwort
- Android: OpenKeychain unterstützt Yubikey Neo (NFC)
- Nutzung PGP-Key als SSH-Key (gpg-agent als ssh-agent)
- Keys offline erzeugen, im Alltag nur die OpenPGP-Karte verwenden

Bullshit made in Germany [5]

E-Mail made in Germany

Aktivierung von SSL/TLS zwischen den Mail-Servern der beteiligten (deutschen) Provider

DE-Mail, E-Postbrief, ...

Marketingkampagne zur Einführung der Briefmarke für E-Mail

Schlandnet

Die Telekom ist schuld!

[5] http://media.ccc.de/browse/congress/2013/30C3_-_5210_-_de_-_s
-_201312282030_-_bullshit_made_in_germany_-_linus_neumann.html

Was Ihr sonst noch so wissen wollt...

Hier ist jetzt Platz für Fragen und Antworten zum Thema

- - -

Diese Vortragsfolien gibt es (ungekürzt) auch zum Download unter

`https://wiki.ctdo.de/vortraege/gnupg`

- - -

- - -

Links zum selber Nachlesen

Links zum Thema:

- http://www.chaostreff-dortmund.de
- http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung
- http://de.wikipedia.org/wiki/Pretty_Good_Privacy
- http://de.wikipedia.org/wiki/OpenPGP
- http://de.wikipedia.org/wiki/Gnupg
- http://de.wikipedia.org/wiki/Alice_und_Bob
- http://de.wikipedia.org/wiki/Web_of_trust
- http://de.wikipedia.org/wiki/Schl%C3%BCsselserver
- http://tools.ietf.org/html/rfc4880

Links zum selber Nachlesen

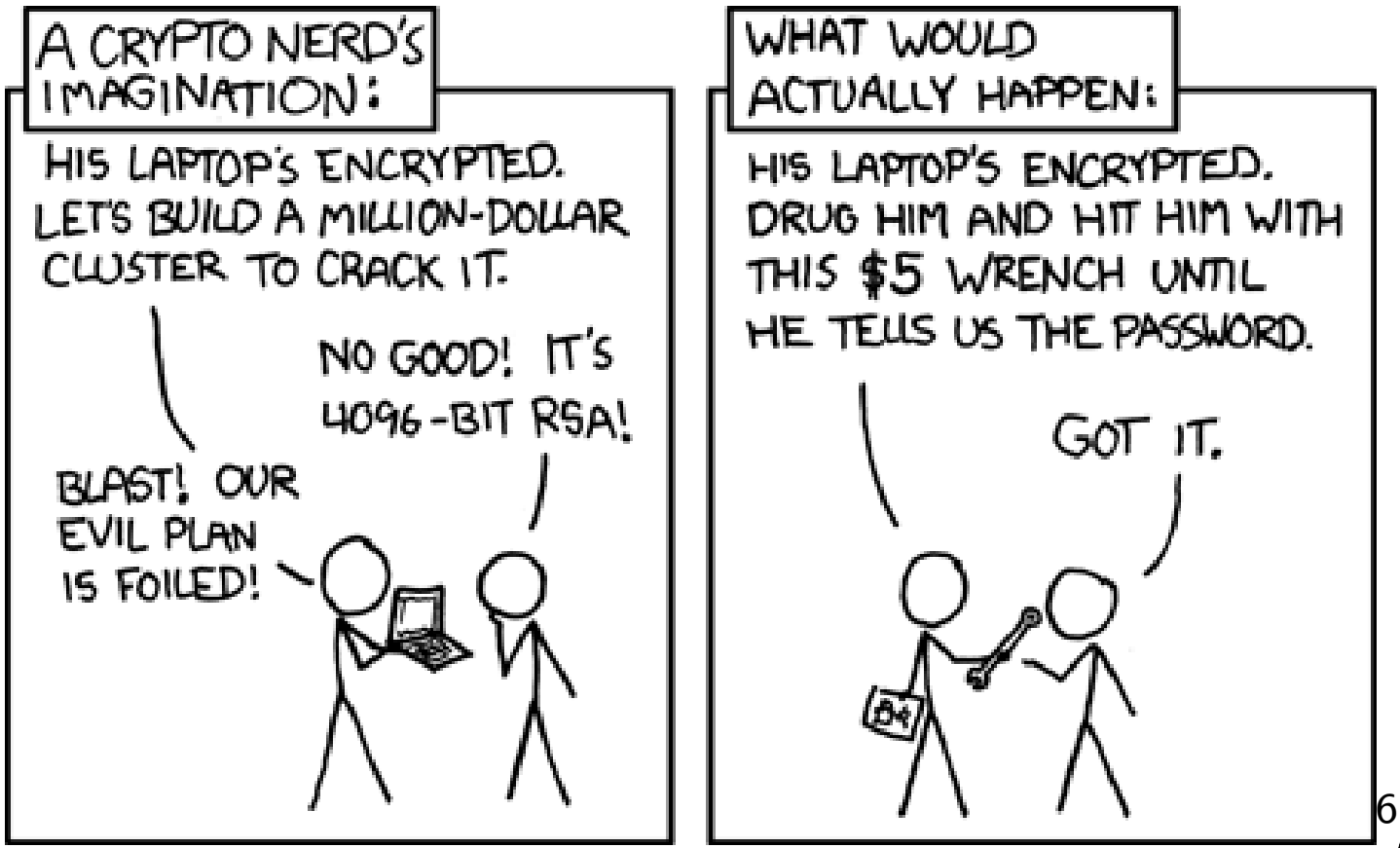
Links zu OpenPGP Smart Cards:

- http://g10code.com/p-card.html
- http://blog.josefsson.org/2014/06/23/offline-gnupg-master-key-and-subkeys-on-yubikey-neo-smart
- http://shop.kernelconcepts.de/
- https://www.yubico.com/products/yubikey-hardware/yubikey-neo/

Danke für Eure Aufmerksamkeit

Danke fürs Zuhören!

Nachwort



[6]

[6] https://xkcd.com/538/