Piratenpartei Deutschland
Landesverband Rheinland-Pfalz

Sichere Verschlüsselung von Emails

Ingo Höft, 9. April 2014

PIRATEN PARTEI

Übersicht

1. angestrebtes Ziel
2. ein antikes Beispiel
3. Prinzip
4. praktische Handhabung
5. ist der Schlüssel echt?
6. etwas zur NSA
7. verwendbare Programme
8. benutzte Programme
9. Einrichtung

angestrebtes Ziel

- starke Verschlüsselung
- Ende zu Ende Verschlüsselung
- keine Vermittler
- ausschließlich vom Anwender kontrolliert
- Standardeinstellung verschlüsseln und unterschreiben
- einfache Handhabung

ein antikes Beispiel

- Schlüssel = Dicke des Stabes
- gemeinsames Geheimnis
- zusätzlich als Gürtel versteckt tragbar

Quelle: https://de.wikipedia.org/wiki/Skytale

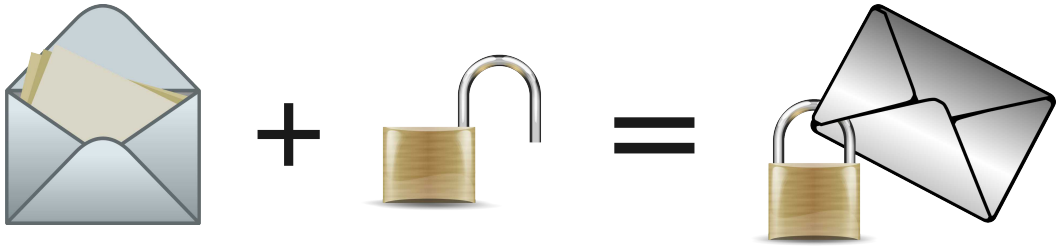
Prinzip

mein Schlüsselpaar

öffentlicher Schlüssel

privater Schlüssel

verschlüsseln
kann jeder

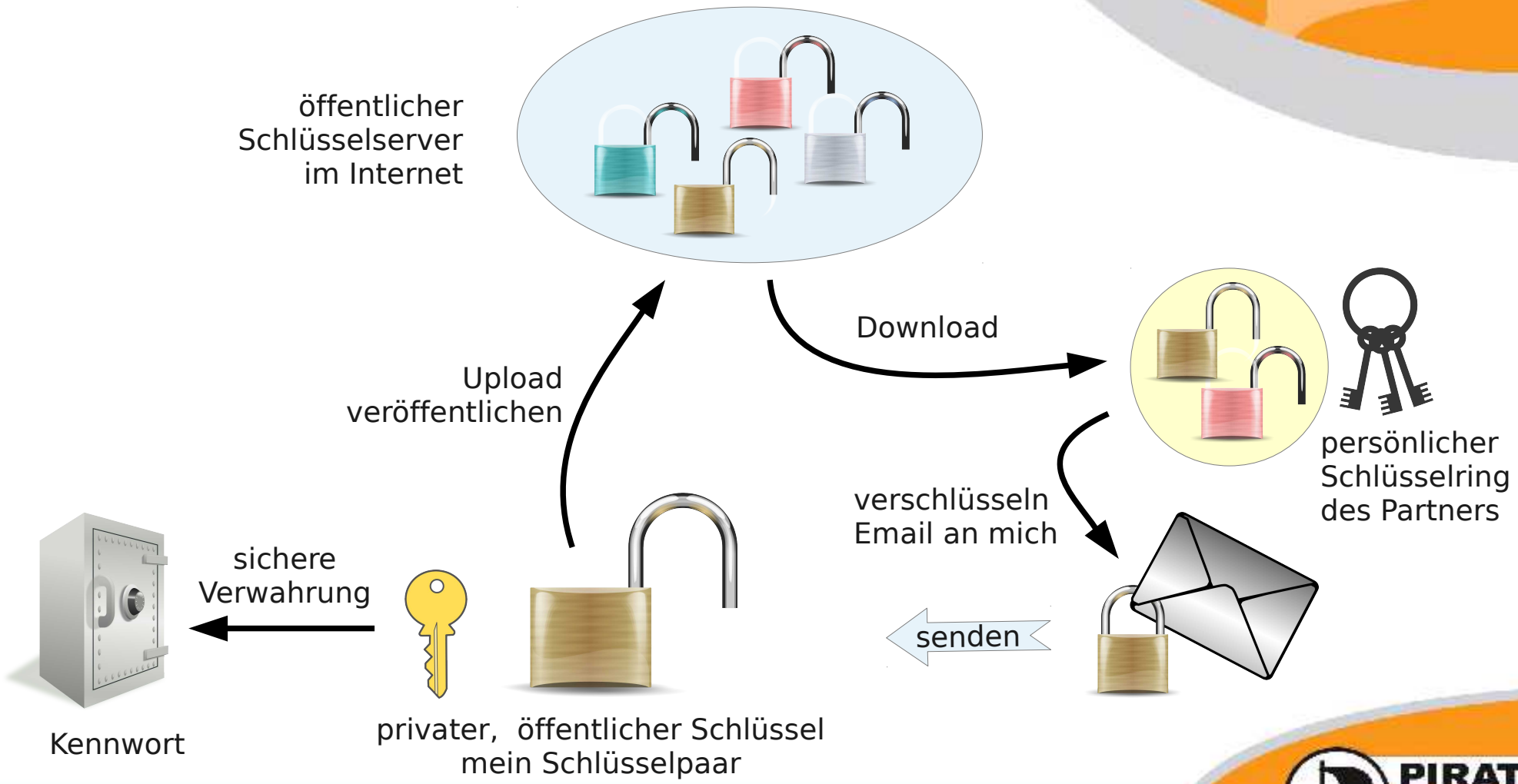


entschlüsseln
kann nur ich

Quelle: http://www.dkruse.de/dokumente/netzwerke/Sicher3_Asymm_Verschluesselung.pdf

praktische Handhabung

Piratenpartei Deutschland
Landesverband Rheinland-Pfalz



Ist der Schlüssel echt?

Problem: woher weiss ich, ob der öffentliche Schlüssel wirklich von der genannten Person ist?

Lösung: jeder, der die Person kennt und genau weiss, dass es sein Schlüssel ist, bestätigt dies per Unterschrift an dem öffentlichen Schlüssel

- Man lässt sich den Fingerabdruck vom Schlüsselbesitzer geben, aber nicht per Mail!
- Man vergleicht den Fingerabdruck mit dem Fingerabdruck des obskuren öffentlichen Schlüssels
- Stimmen die überein, so unterschreibt man den öffentlichen Schlüssel mit seinem eigenen privaten Schlüssel („signieren“)
- Man kennzeichnet für sich den fremden öffentlichen Schlüssel in seinem Schlüsselring als „vertraut“
- Je mehr Unterschriften ein öffentlicher Schlüssel hat, desto glaubwürdiger ist er

etwas zur NSA

Die NSA (National Security Agency):

- speichert alle Emails und Telefonate
- verlangt die Herausgabe aller privaten Schlüssel von amerikanischen Firmen
- verlangt die Herausgabe aller bekannten Sicherheitslücken, auch die unveröffentlichten von amerikanischen Firmen
- hat freien Zugang zu allen Daten von Facebook, google, Apple, Microsoft und andere mit eigener spezieller Software, die die Firmen installieren müssen
- kann stark verschlüsselte Emails **nicht** entschlüsseln!

Grundlage für die Verpflichtung der amerikanischen Firmen ist das Gesetz „USA PATRIOT Act“

verwendbare Progamme

- Outlook Express
- Outlook
- Apple Mail
- web Mailer
- ???

benutzte Programme

- Thunderbird
  - quelloffen
  - kostenlos
  - nicht kommerziell
  - läuft auf allen größeren Betriebssystemen
- GnuPG
  - quelloffen
  - sehr hoher Sicherheitsstandard
- EnigMail
  - quelloffen
  - sehr gute Integration von Thunderbird und GnuPG

ein kurzer praktischer Einblick

gibt es noch Fragen?