LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

IT-Sicherheit und Datenschutz

Vorlesung Probestudium

Marianne Busch
busch@pst.ifi.lmu.de

Gliederung

1. **Begriffe**
2. Gegenmaßnahmen zum Abhören oder Verändern des Netzverkehrs
   - Datenverschlüsselung und Signatur
   - SSL/TLS Verbindungen (https)
3. Gegenmaßnahmen zum Datendiebstahl beim Provider oder auf eigenen Geräten
   - Sichere Passwörter und zusätzliche Maßnahmen
   - Datenverschlüsselung auf dem eigenen Computer
   - Schutz von Smartphones
   - Daten über Verhalten und Interessen
4. Social Engineering Angriffe abwehren

IT-Sicherheit: Angriffsziele

Netze: Sniffen, Spoofen, Denial of Service, ...

Web-Anwendungen und Datenbanken:

Cross-Site Scripting (XSS), SQL-Injection, ...

Gute Erklärungsvideos:
https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series

Server bzw. PCs: Viren, Würmer, Trojaner, ...

Abhilfe: aktuelle Updates installieren, Virenscanner, keine fremden Dateien öffnen, Checksummen nach Downloads überprüfen, ..

Benutzer: Phishing, Spamming, ...

Schutzziele der IT-Sicherheit

- **(Daten-) Integrität (engl. integrity)**
  - Schutz vor unautorisierter und unbemerkter Modifikation von Daten
- **(Informations-) Vertraulichkeit (engl. confidentiality)**
  - Schutz vor unautorisierter Informationsgewinnung
- **Verfügbarkeit (engl. availability)**
  - Schutz vor unbefugter Beeinträchtigung der Funktionalität von Diensten etc.
- **Verbindlichkeit (engl. accountability / non-repudiation)**
  - Schutz vor unzulässigem Abstreiten durchgeführter Handlungen
- **Authentizität (engl. authenticity)**
  - Nachweis der Echtheit und Glaubwürdigkeit der Identität eines Objekts/Subjekts
- **Privatheit / Datenschutz (engl. privacy)**
  - Schutz der personenbezogenen Daten, Schutz der Privatsphäre, Gewährleistung des informationellen Selbstbestimmungsrechts

Warum Datenschutz?

Wer schützt meine Daten?

Post-Privacy-Zeitalter?

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."

Europäische Menschenrechtskonvention Art. 8 Abs. 1

Bürger hat laut **Bundesdatenschutzgesetz** folgende Rechte:

(gem. § 6 Abs. 1 BDSG – Auszug)

- Auskunft darüber, ob und welche personenbezogenen Daten über sie gespeichert sind & Quelle & Verwendungszweck
- Berichtigung von falschen personenbezogenen Daten
- Löschung oder Sperrung ihrer Datensätze.

https://de.wikipedia.org/wiki/Bundesdatenschutzgesetz

Authentifikation (engl. Authentication)

Begriffe (Duden)

- authenti**sieren**: rechtsgültig machen, (sich selbst) glaubwürdig machen
- authenti**fizieren**: Echtheit bezeugen, beglaubigen, einen Benutzer identifizieren

„Ein Benutzer authentisiert sich am Server; der Server authentifiziert den Benutzer“

Ziel der Authentifikation:

Identifizierung von Subjekten und Nachweis der (eigenen) Identität

Autorisierung (engl. Autorization)

Vergabe / Spezifikation von Rechten

Ziel der Autorisierung:

Zugriffskontrolle: Durchsetzung der spezifizierten Rechte

„Zugriff hat nur derjenige dem das erlaubt ist.“

Wiederholung wichtiger Begriffe

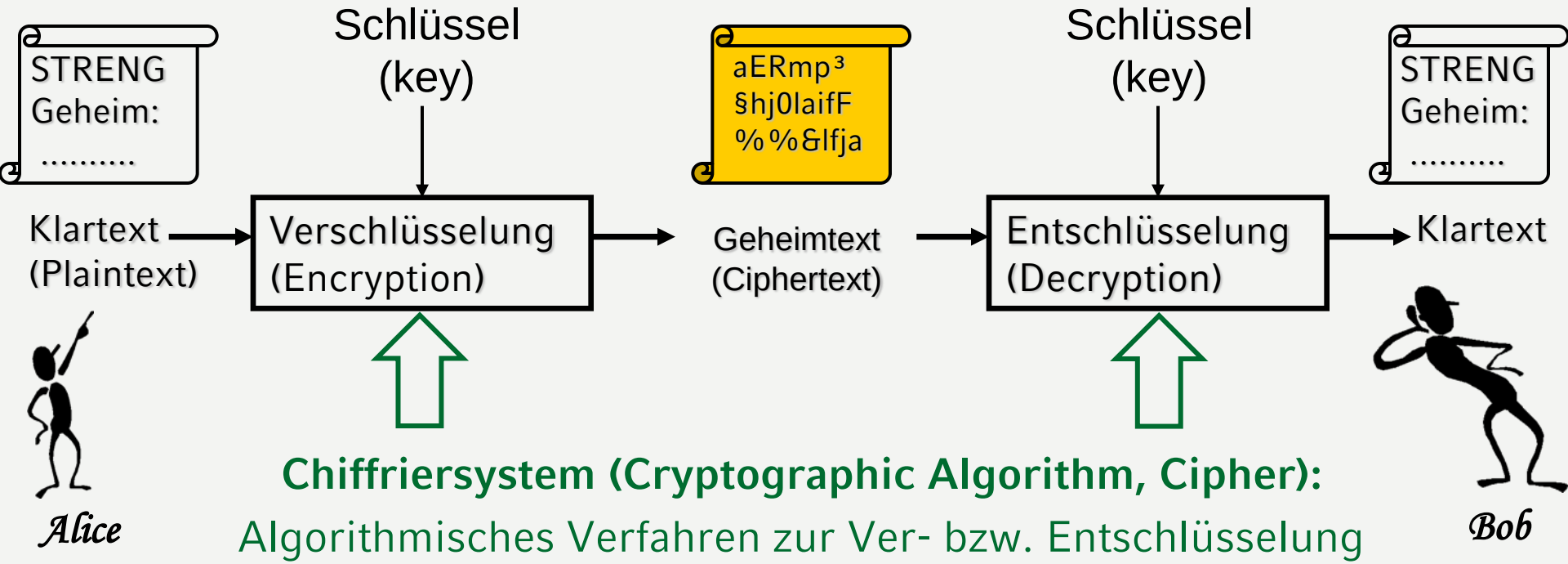
- **Integrität**
- **Vertraulichkeit**

- **Authentifikation**
- **Autorisierung**

Gliederung

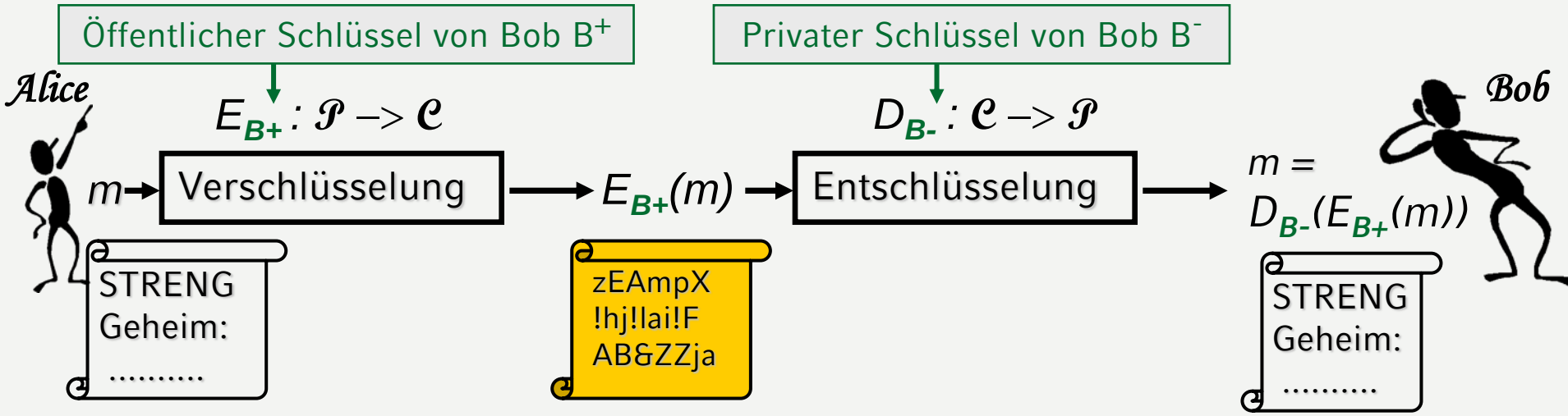
1. Begriffe
2. **Gegenmaßnahmen zum Abhören oder Verändern des Netzverkehrs**
   - Datenverschlüsselung und Signatur
   - SSL/TLS Verbindungen (https)
3. Gegenmaßnahmen zum Datendiebstahl beim Provider oder auf eigenen Geräten
   - Sichere Passwörter
   - Zusätzliche Maßnahmen, z.B. Google 2-step, mobileTAN
   - Datenverschlüsselung auf dem eigenen Computer
   - Schutz von Smartphones
4. Social Engineering Angriffe abwehren

Symmetrisches Verschlüsselungsverfahren:
Ver- und Entschlüsselung mit gleichem Schlüssel



Chiffriersystem (Cryptographic Algorithm, Cipher):
Algorithmisches Verfahren zur Ver- bzw. Entschlüsselung

Asymmetrisches Verschlüsselungsverfahren:
Verschlüsselung mit öffentlichem Schlüssel
Entschlüsselung mit privatem Schlüssel



Asymmetrisches Verschlüsselungsverfahren:
Verschlüsselung mit öffentlichem Schlüssel
Entschlüsselung mit privatem Schlüssel

Jeder Partner P besitzt **Schlüsselpaar (P^+, P^-)** aus

- persönlichem, geheim zu haltendem Schlüssel (***private key***)
- und öffentlich bekannt zu gebendem Schlüssel (***public key***)

Protokoll (E = Verschlüsselungsfunktion, D = Entschlüsselungsfunktion):

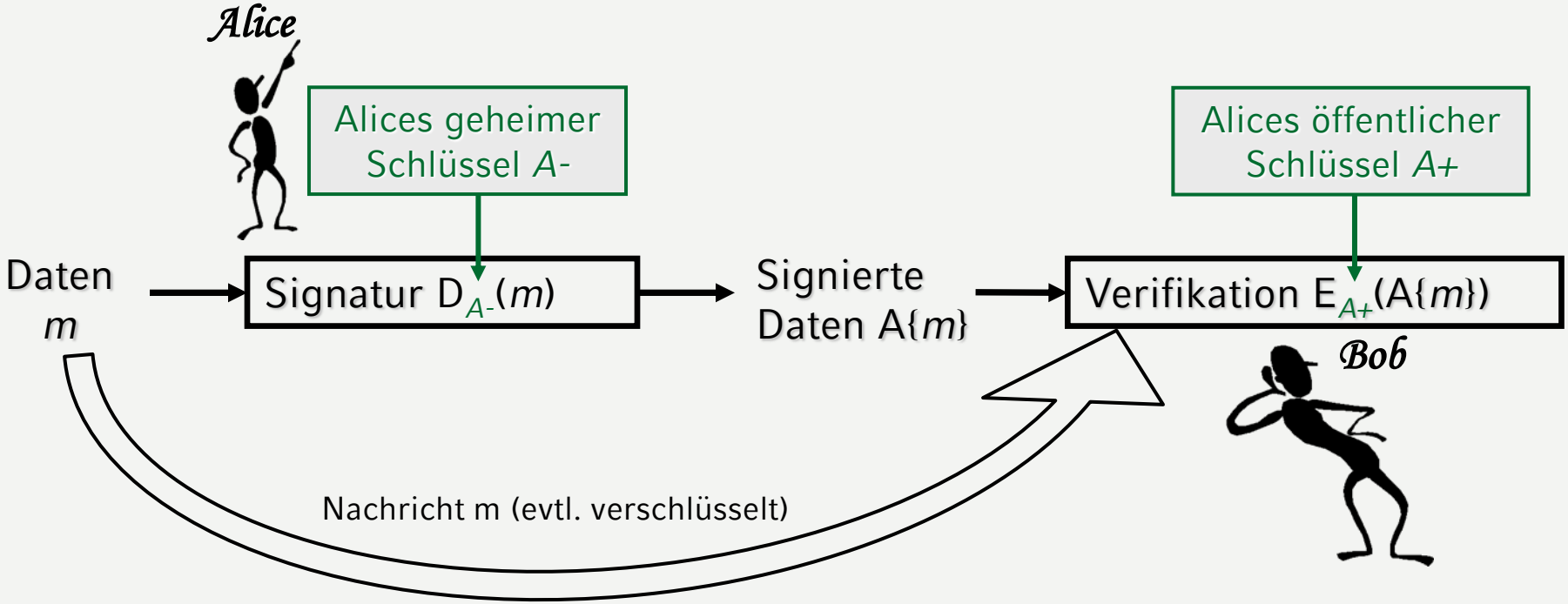
1. Alice und Bob erzeugen sich Schlüsselpaare: $(A^+, A^-), (B^+, B^-)$
2. Öffentliche Schlüssel werden öffentlich zugänglich gemacht
3. Alice will Nachricht *m* an Bob senden; dazu benutzt sie Bobs öffentlichen Schlüssel $E_{B+}(m) = c$
4. Bob entschlüsselt die verschlüsselte Nachricht *c* mit seinem privaten Schlüssel:

$$D_{B-}(c) = D_{B-}(E_{B+}(m)) = m$$

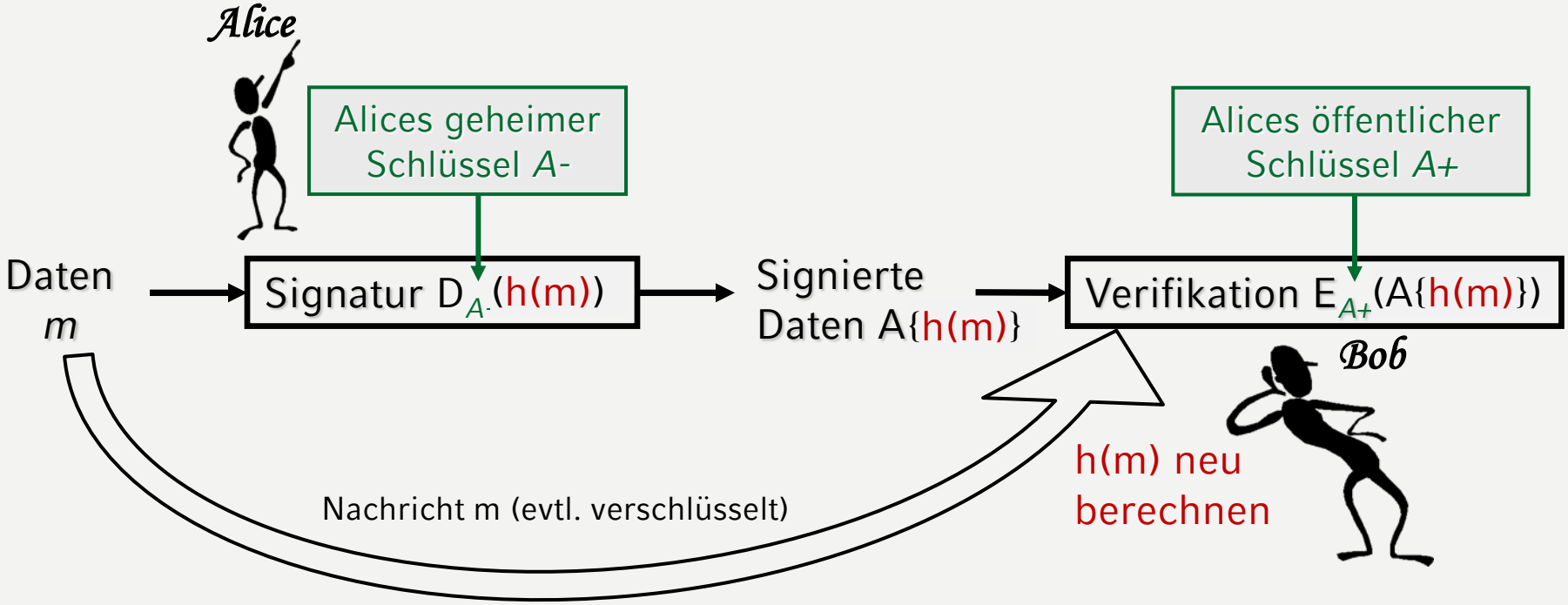
Asymmetrisches Kryptosystem: Digitale Signatur (Unterschrift)

Alice „signiert“ Nachricht *m* mit ihrem privaten Schlüssel $A\{m\} =_{def} D_{A-}(m)$

Jeder kann die Signatur mit Alices öffentlichem Schlüssel überprüfen



Asymmetrisches Kryptosystem: Digitale Signatur (Unterschrift)



Asymmetrische Verfahren sind im Vergleich zu symmetrischen sehr langsam.

Nur Fingerabdruck **= kryptographischer Hash-Wert *h(m)*** der Daten wird signiert.

OpenPGP Standard (z.B. für E-Mails genutzt)

OpenPGP basiert auf hybridem Kryptosystem
(symmetrisch & asymmetrisch)

1. Sitzungsschlüssel erzeugen
   und Text damit verschlüsseln
2. Sitzungsschlüssel mit öffentlichem Schlüssel verschlüsseln

Im Gegensatz zu OpenPGP:
S/MIME-Protokoll verwendet X.509-Zertifikate

Beispiel: E-Mail Verschlüsseln / Signieren mit Enigmail für Thunderbird (GnuPG)

Thunderbird

https://www.mozilla.org/de/thunderbird/

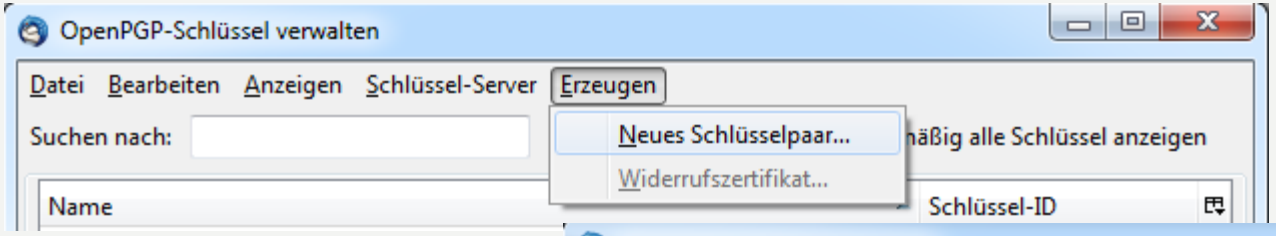
GnuPG

http://www.gnupg.org/ (Windows: http://www.gpg4win.org/)

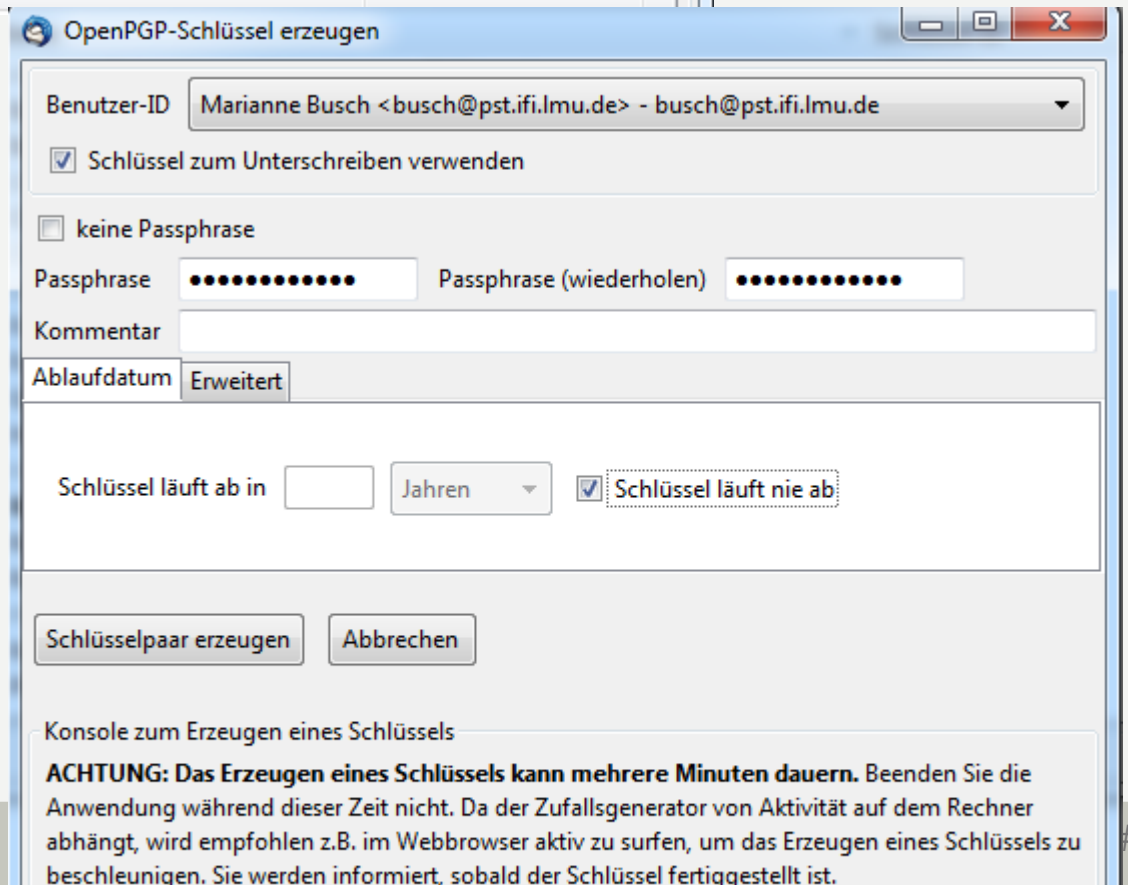
Enigmail

https://addons.mozilla.org/de/thunderbird/addon/enigmail/

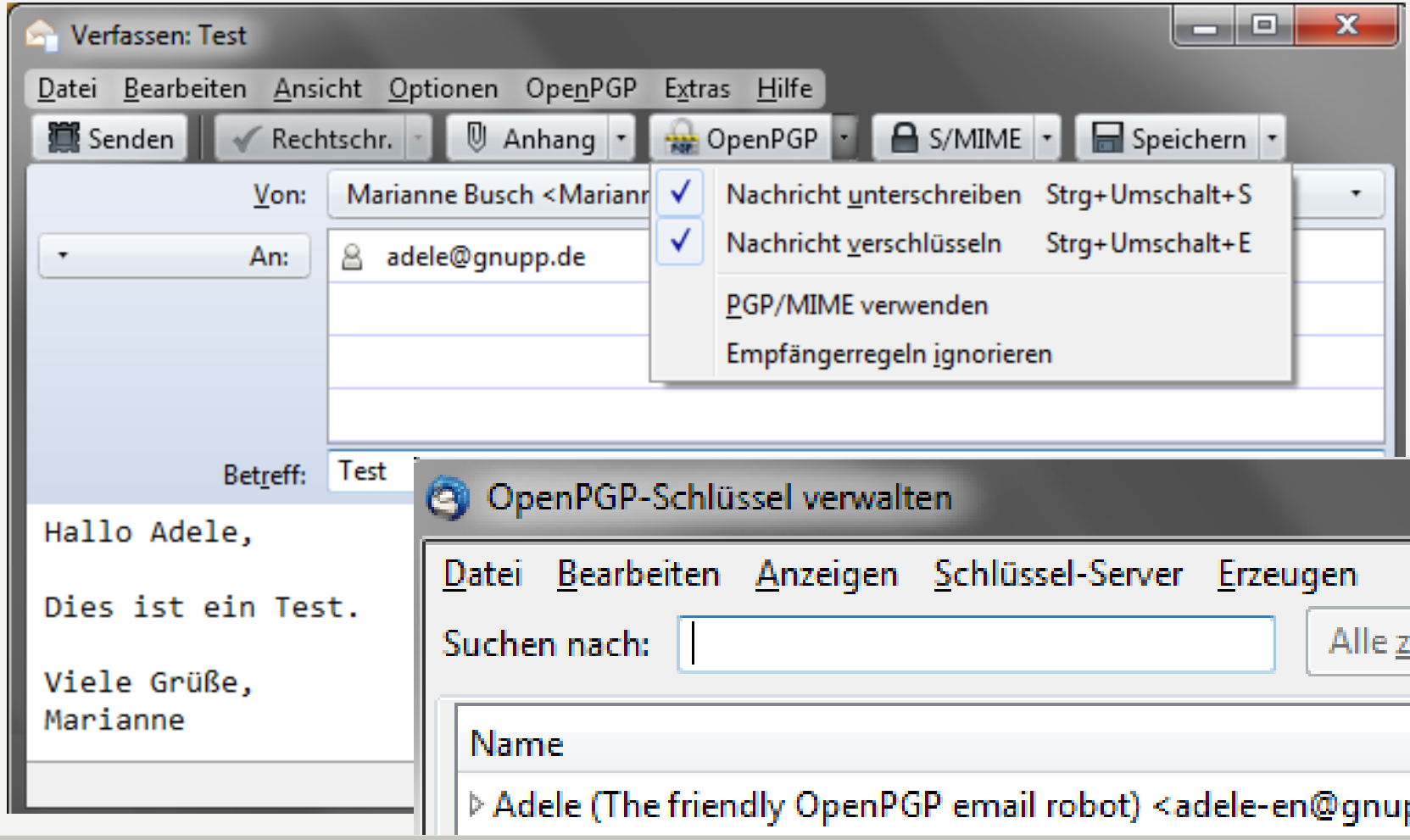
OpenPGP / Schlüssel verwalten



Neues Schlüsselpaar



Testen z.B. mit Mailbot Adele (adele@gnupp.de)



Verschlüsselte & signierte Nachricht

-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.11 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEOAysxYodivb/UEAP+NdUnWjenTg1VutPRVJjPP45UiZbA4A3L5ZBKLqwLEsHE
rVSgF/1nwETqr4K65VuRfx2yQ3JOdCL1UD6y4EiNkrqtP66zwHJWseIx1EayycYc
kxpBfHkdr33rTM1bDEirF7js1G5qUyl9DdfWr/38ZqAxh0/EI803cH0t462eVvYD
/AIGMEDR7L+eAh54OKc6fpxWSIjIgQaBAVRnQ2WcBcFXjd9gMgAWIKisHgjZ+KWg
5YmXTGj4Y41s9a/JQa90MCU/vfTkpvyGQFyAWR2Zor8Kn5umnEuEfPdvX8fAjyyl
xThEAaGwdlnKj5kCXIABOMafseGMdoLa81oo66aUmcy9hQIOA2gn3nApyXd4EAgA
gegYZhZnHMJyNe/pqCVszFfQ02heiIDpqxDpn3aOGOkWPQKMWRnH0wWKRy/lo9GZ
3mYFJzy/SgI9bfLSeJg/Ehr+NMcur86mHNHUSksS9AIYL3fwoCMhAFyI9LFUIT9r
Cyq8sXgZ/uyzlsA0+l1fVouGk52Vt4/MwAjA0DZhhC7Pvyd6cUq9FIMGPzpkWDH0
DAmn7mEnv7H41wBaH8JFp+0DVaPk5Ect8w+zWtg9yqox2xyhzM7E7Ap7e5sCbOqz
KDRPMVOFZOMkJkU4DIMPk0IOri1qpAhTty0M3QGeeDAOyngN3fdNNZA7DHDpV1Kk
y6HRFiI9Yn3g8mhL87PADwgAIkN1JFrHJmTQzra89yXjJaY0uzHG6fjP5oHTRIoi
4ixFRKbvXQ6t2ZxzRUUogd0QClzxi3gNfdj8K9Hi5btnusL9dEWXpHVOBiVrkXqe
2cSUwDxTBMyTrGmTTNdGtxb0xOKgQIj1dxNRTW8ekqWyW12Mm0UWfNj2kI5sbLbh
G7eKigx3WPzbm3q/SBJ52mJw3PrsIpcsBmUCHk6Uy7abKrKVqFW6v/aiGPxZus8P
HoIDU8yxm/W3Gw12VGCS7ZYib0gxb8fLJDrG9E8fUOP1L5v3OynGpyOC0dmO7vd6
XJl+Lepe953jC6Xyo4FkAnddAL++H0oAdk3weLdtND/ITtLABgE5djN4Rp2ZiVrq
bVdXq9z1LXXBuRJzL7mWlUEg4O31IdHYvADstrGmppJ2oJMrV4qMshVMaT51JxFR
INs+zvuH7Y/n0FokZEvk39oPFLUnlyXWjFWLkPou7EjN+6ORUhePAczN/Q4sLB2V
eX3XrU4gQwjXB4dYSrcGgVeIRf8AMe36+mgbNTjeQ03SL/APaOX2xScLbQmPy+Rg
cAo/fHIGSj4EcoIRE547qEO07FSxhFQ+7pP6OMGNg6AJypvAIO1O/7+23Q==
=WE+W
-----END PGP MESSAGE-----

PGP Public Key Server, z.B. http://pgp.mit.edu/

Beispiele für Signaturen:

- Heise Krypto-Kampagne
  http://www.heise.de/security/dienste/Krypto-Kampagne-2111.html
- CAcert
  http://www.cacert.org/

Assurer-Suche bei CAcert

Please enter your town or suburb name, followed by region or state or province and then the country (please separate by commas)
eg Sydney, New South Wales, Australia

This is an AJAX form which depends heavily on javascript for auto-complete functionality and while it will work without javascript the usability will be heavily degraded.

Maximum Distance: 10km

Location: Augsburg, Bayern, Germany Go

Augsburg, Bayern, Germany	105325
Augsberg, Bayern, Germany	105323
Augsburg, Schleswig-Holstein, Germany	105324
Augsburg, Mpumalanga, South Africa	105326
Augsburg (Fayette), Illinois, United States	2115725
Augsburg (Pope), Arkansas, United States	2086279
Augsbuur, Friesland, Netherlands	105327
Augsbuurt, Friesland, Netherlands	105328
Augsbuurt-Lutjewoude, Friesland, Netherlands	105329

CAcert.org
- Go Home
- Logout

+ My Details
+ Email Accounts
+ Client Certificates
+ GPG/PGP Keys
+ Domains
+ Server Certificates
+ CAcert Web of Trust
  - About
  - Find an Assurer
  - Rules
  - Assure Someone
  - Trusted ThirdParties
  - Training

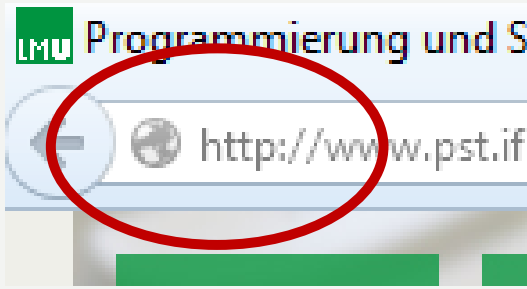
Eigentlich einfach, wird trotzdem nicht oft benutzt
(auch nicht oft von Firmen)

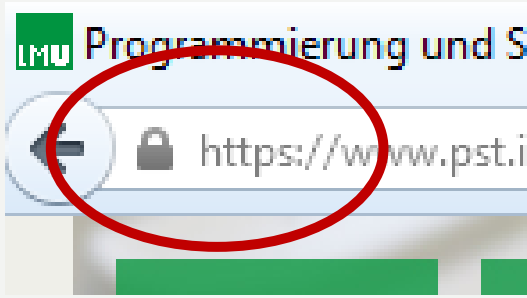
(Geringer) technischer Aufwand vs. Bequemlichkeit?

E-Mail = Postkarte. Kann jeder auf dem Übertragungsweg lesen
(„meine Mails interessieren doch keinen..“
➔ erleichtert Phishing: enthalten Infos über andere)

Unverschlüsselte HTTP-Sitzungen erlauben:

- Abfangen von unverschlüsselten Cookies
- Ausnutzen zum Einloggen





Lösung: SSL/TLS verwenden!

- URLs mit https benutzen
- Browser-Plugin dass automatisch auf https-Version umleitet, z.B. https://www.eff.org/https-everywhere

Schutz vor Angriffen auf Netzwerkverbindungen

- E-Mails verschlüsseln: Vertraulichkeit
  (Spion kann sie nicht lesen)
- E-Mails signieren: Integrität
  (Niemand kann sie verändern)
- Im Internet möglichst sichere Verbindungen verwenden
  (auf https und gültiges Zertifikat achten)

Gliederung

1. Begriffe
2. Gegenmaßnahmen zum Abhören oder Verändern des Netzverkehrs
   - Datenverschlüsselung und Signatur
   - SSL/TLS Verbindungen (https)
3. **Gegenmaßnahmen zum Datendiebstahl beim Provider oder auf eigenen Geräten**
   - Sichere Passwörter und zusätzliche Maßnahmen
   - Datenverschlüsselung auf dem eigenen Computer
   - Schutz von Smartphones
   - Daten über Verhalten und Interessen
4. Social Engineering Angriffe abwehren

Google als Passwort-Cracker

Häufig wird MD5 als Hash-Funktion verwendet

- Google liefert zu Hash-Werten beliebter Passwörter den zugehörigen Klartext (oder auch nicht...)

Beispiele:

- md5(admin) = 21232f297a57a5a743894a0e4a801fc3
- md5(abc123) = e99a18c428cb38d5f260853678922e03

Es gibt Datenbanken: Passwort – Hash des Passworts für häufige Kennwörter und Wörterbucheinträge

➔ nie existierende Wörter verwenden!

Vermeidung?

"*The password must be impossible to remember and never written down.*"
(Richard E. Smith: "The Strong Password Dilemma")

gutes Gedächtnis oder Toolsupport

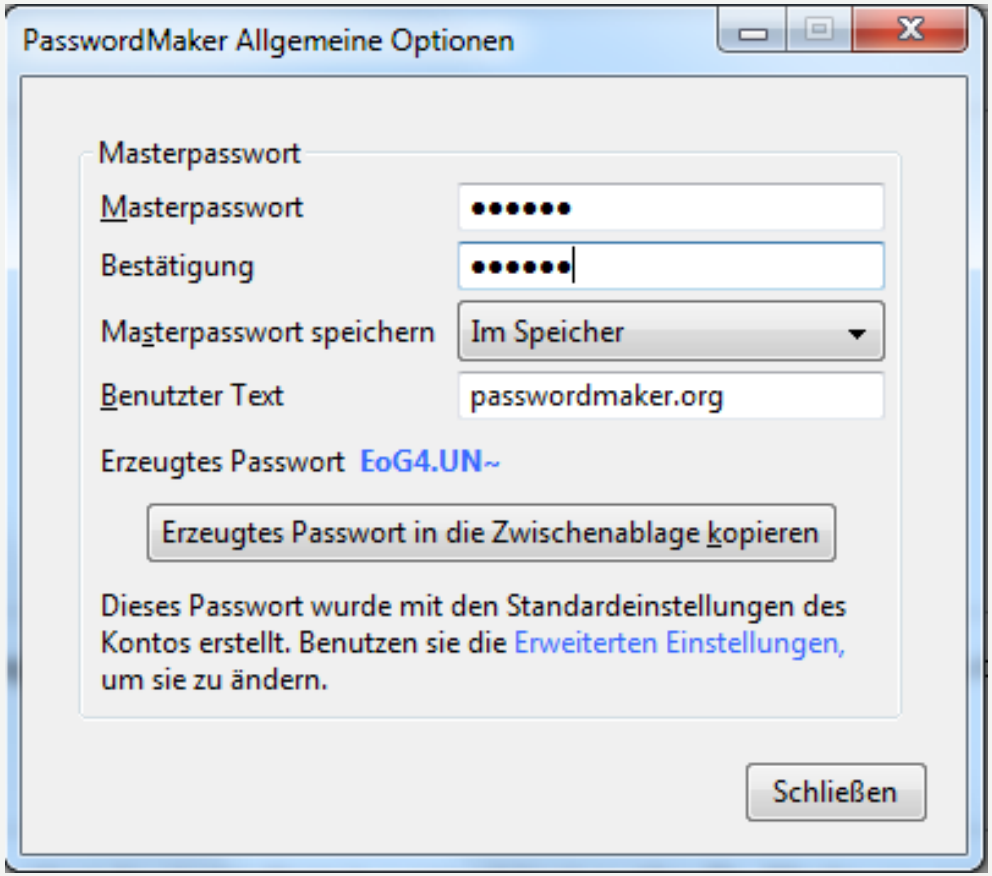
- Lange Sätze bilden: „*Karl kauft über 7 Kilo frisches &bst und kocht daraus viele Gläser leckere Marmelade*" ➔ Kkü7Kf&ukdvGIM
  - Passwortknacker rechnen mit Leetspeak (s. c't 2/13)
  - Lügen bei Kontrollfragen für Passwort-Reset
  - Alles persönliche in Kennwörtern verfälschen (z.B. kein Geburtsdatum)
  - Anderes Kennwort für jeden Dienst

gH31m+137

- Tool: z.B. PasswordMaker http://passwordmaker.org/

PasswordMaker http://passwordmaker.org/

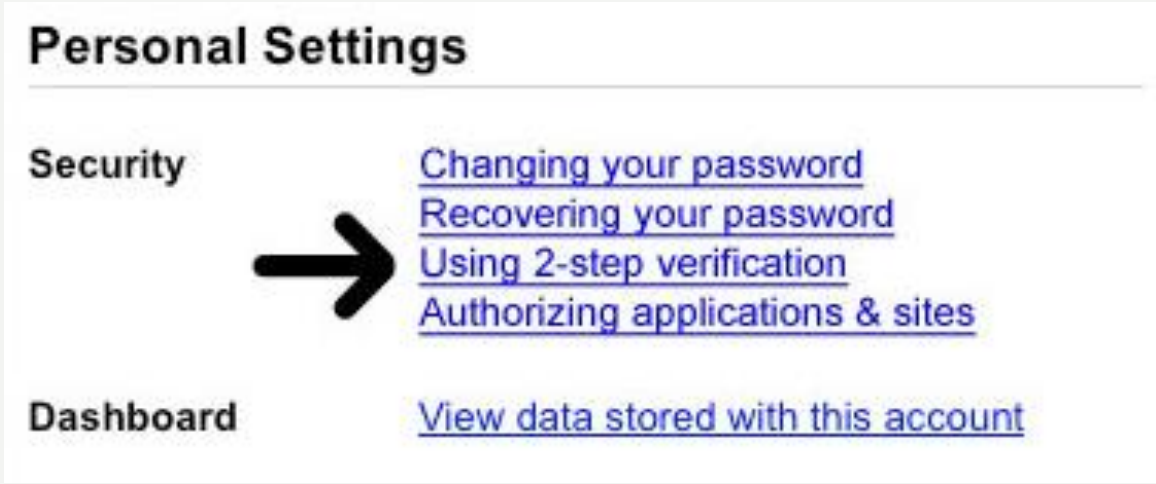
Erzeugt aus Masterpasswort + URL (beliebigem Text) ein Kennwort



- Nicht nur ein Masterkennwort verwenden!
- Manche Seiten akzeptieren nicht alle Sonderzeichen.
- URL als Text reicht nicht wenn mehrere Accounts bei einem Anbieter existieren

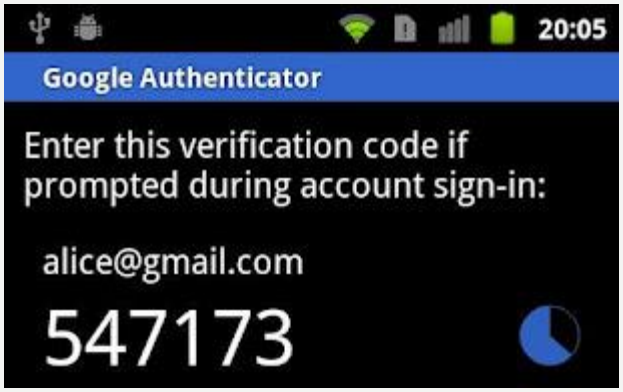
Ziel: Nicht nur Passwort, sondern auch Bestätigungscode eingeben

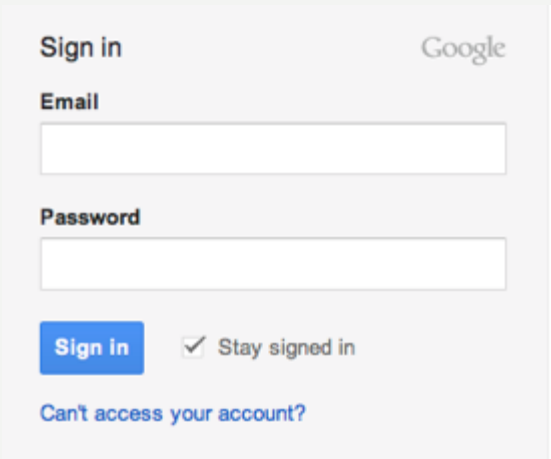
Einrichten



Verwenden

- Am Smartphone Nummer ablesen
- In Web-Formular eingeben





Verwenden

- Am Smartphone Nummer ablesen
- In Web-Formular eingeben

Anwendungsspezifische Passwörter

Zusätzliche Authentifizierung, erschwert man-in-the-middle attacks

TAN = Transaktionsnummer = Einmalpasswort z.B. für Überweisung

iTAN

- durchnummerierte TANs auf einer Liste (wird zugeschickt),
  eine bestimmte davon muss dann eingegeben werden

mobileTAN (per SMS)

1. Man gibt eine Handynummer an und verifiziert sie, indem man eine Nummer abtippt, die per SMS gesendet wurde
2. Bei folgenden Überweisungen fordert man eine mobileTAN an und erhält eine SMS aufs Handy:
   „Die mobileTAN für Ihre Überweisung an Konto 123, BLZ 123 über EUR 123 lautet: 123456“
   Achtung: Schadsoftware befällt gerne Handy **und** PC!

Wer hat Zugriff?

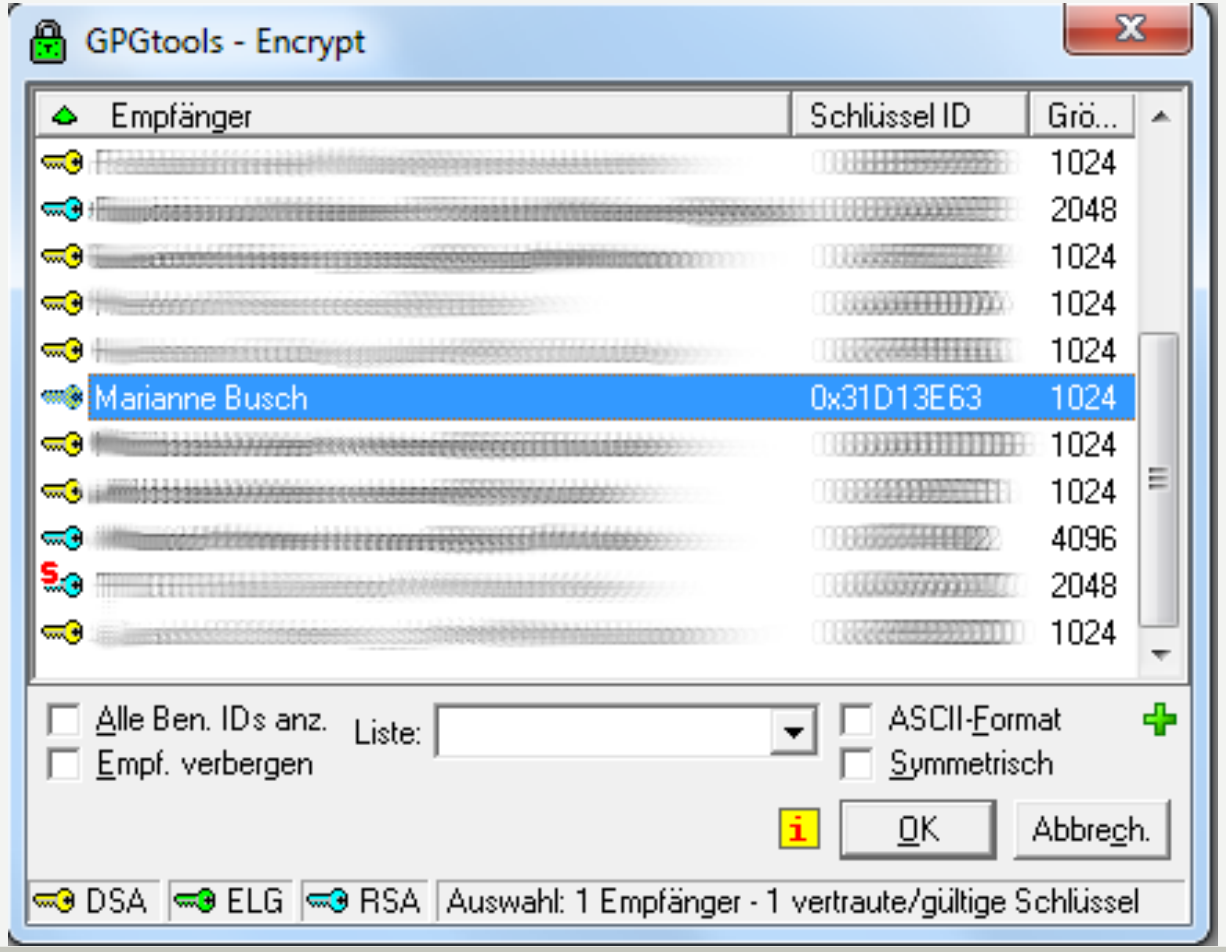
- Freunde?
- Kollegen?
- Spaßvögel?
- Trojaner?
- Diebe?

Auf was?

- Lokale Dateien (Kontoauszüge, Rechnungen, E-Mails, Urlaubsfotos, …)
- Kennwörter für Web-Dienste
- Logfiles, …

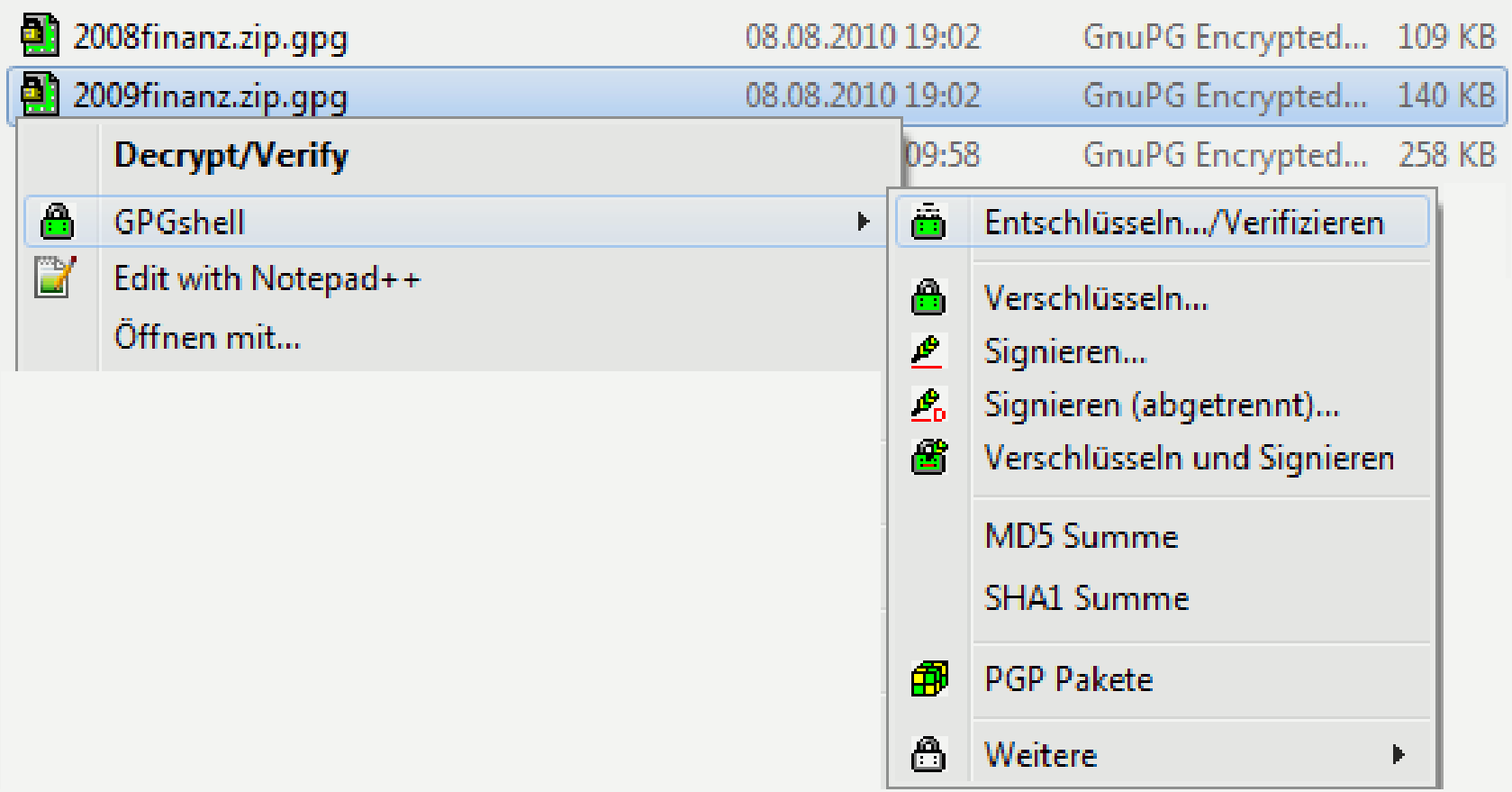
Verschlüsseln einzelner Dateien z.B. mit gpg4win

http://gpg4win.de



Entschlüsseln einzelner Dateien z.B. mit gpg4win

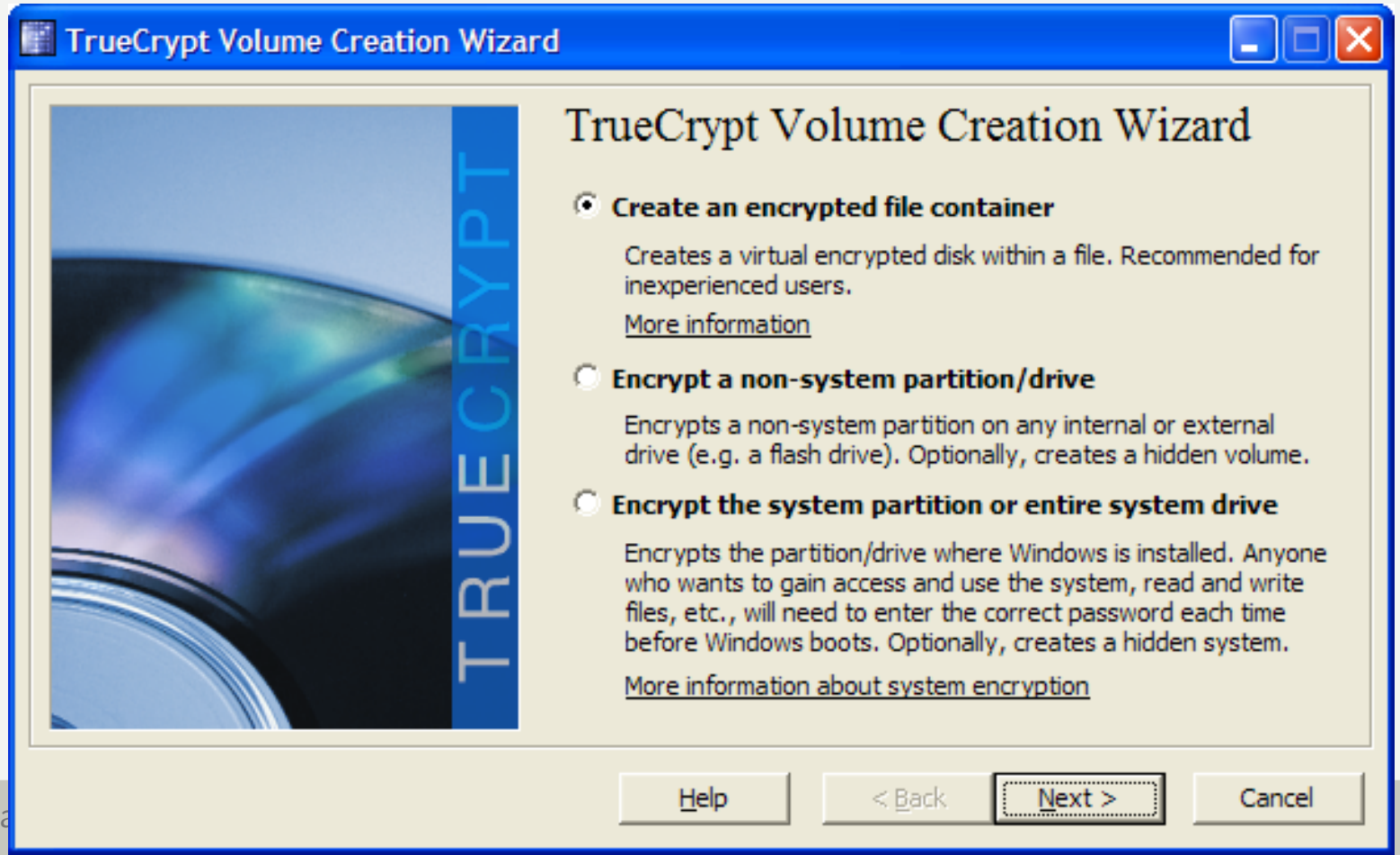
http://gpg4win.de



Verschlüsseln einzelner Dateien z.B. mit OpenPGP

Verschlüsseln ganzer Partitionen z.B. mit TrueCrypt

http://www.truecrypt.org/



Kennwörter eingeben ist lästig

Smartphones werden leicht geklaut

Synchronisieren über das Web ist bequem

Google & Co kennen unsere Kalender, Adressen, Aufgaben, …

Apps ausprobieren ist praktisch

Sicherheitsrisiken (trotz Virenscanner)

„Android-Spiele enthalten Trojaner“
http://heise.de/-1424081 (01.2012)

App-Klone mit anderem Herstellernamen (z.B. ~Inc.)
ESSOS 2012 Potharaju et al.
„Plagiarizing Smartphone Applications: Attack Strategies and Defense Techniques”

- im besten Fall nur die Google-Werbe-ID geändert
- im schlimmsten Fall Malware

Angriffswelle auf Android-Handys (Spam)
http://www.digital-zeitschrift.de/nachrichten.php?id=1259 (21.12.2012)

Tapjacking: An Untapped Threat in Android
http://blog.trendmicro.com/trendlabs-security-intelligence/tapjacking-an-untapped-threat-in-android/ (14.12.2012)

Neue Android-App will mithören
http://heise.de/-1796828 (04.02.2013)

Android ist hier nur ein Beispiel

Das *Like*-Problem

I-Frame für Like-Button

Cookie und Referer werden an Facebook gesendet

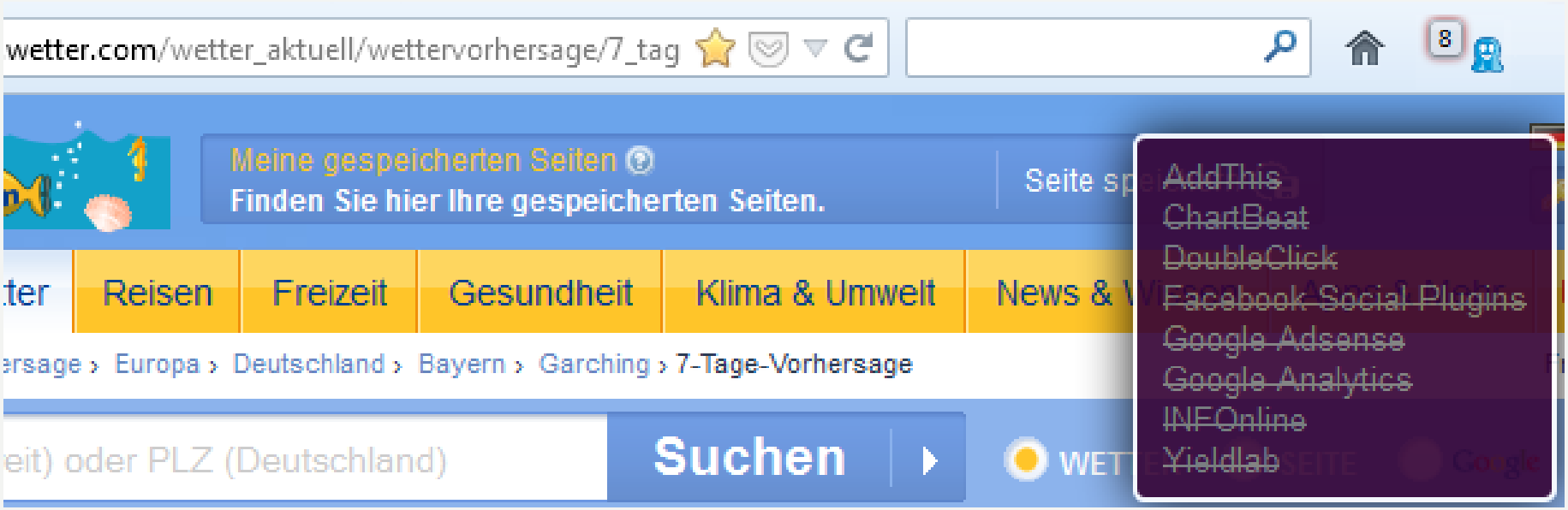
➔ Facebook o.ä. weiß auf welche Seiten man surft
(auch wenn man kein Facebook-Account hat, Browser sind identifizierbar, s. http://panopticlick.eff.org/)

Idee:
2-Klicks für mehr Datenschutz

(von Heise, frei verwendbar:
http://www.heise.de/extras/socialshareprivacy/)

Selbstschutz gegen Tracker

- “Do not track” im Browser aktivieren (für Webseitenbetreiber optional)
- Plugin verwenden, z.B. Ghostery
  http://ghostery.com/



Gliederung

1. Begriffe
2. Gegenmaßnahmen zum Abhören oder Verändern des Netzverkehrs
   - Datenverschlüsselung und Signatur
   - SSL/TLS Verbindungen (https)
3. Gegenmaßnahmen zum Datendiebstahl beim Provider oder auf eigenen Geräten
   - Sichere Passwörter und zusätzliche Maßnahmen
   - Datenverschlüsselung auf dem eigenen Computer
   - Schutz von Smartphones
   - Daten über Verhalten und Interessen
4. **Social Engineering Angriffe abwehren**

Phishing-Angriff

- **Angriff**, der bestehende Geschäfts- und Vertrauensbeziehungen ausnutzt.
- **Vorgehen**: Benutzer werden mit gefälschten E-Mails und Webseiten getäuscht, um sie zur Eingabe vertraulicher Daten zu verleiten.
- **Angriffsziel**: Stehlen der Identität (Authentizitätsproblem)

➔ Heutzutage: Spear-Phishing

s. Technology Review von Nov 2011
http://www.heise.de/artikel-archiv/tr/2011/11/44_kiosk

TR-Artikel: Die 7 tödlichen Schwächen

1. Sex-Appeal
2. Gier
3. Eitelkeit
4. Vertrauen
5. Faulheit
6. Mitgefühl
7. Eile

http://www.heise.de/artikel-archiv/tr/2011/11/44_kiosk

Fragen?

Sicherheitslücken gibt es täglich neue …

… Informatiker werden dringend gebraucht!