

IT-Sicherheit und Datenschutz

Vorlesung Probestudium

Marianne Busch

busch@pst.ifi.lmu.de

<http://www.pst.ifi.lmu.de/Personen/team/busch>





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



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, Virens Scanner, 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)

- **authentisieren**: rechtsgültig machen, (sich selbst) glaubwürdig machen
 - **authentifizieren**: 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. Authorization)

Vergabe / Spezifikation von Rechten

Ziel der Autorisierung:

Zugriffskontrolle: Durchsetzung der spezifizierten Rechte

„ Zugriff hat nur derjenige dem das erlaubt ist.“

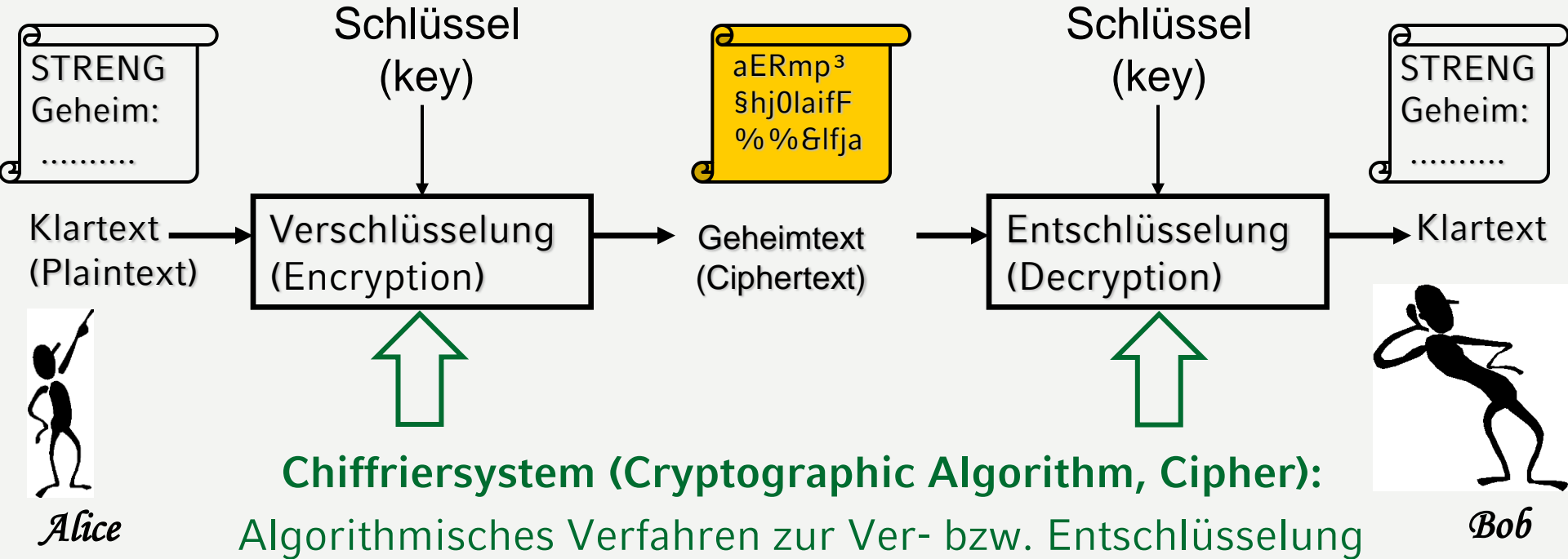


1. Begriffe
2. **Gegenmaßnahmen zum Abhören oder Verändern des Netzverkehrs**
 - Datenverschlüsselung und Signatur
 - SSL/TLS Verbindungen (https)
3. Gegenmaßnahmen zum Datendiebstahl beim Provider oder auf eigenen Geräten
 - Sichere Passwörter
 - Zusätzliche Maßnahmen, z.B. Google 2-step, mobileTAN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



Symmetrisches Verschlüsselungsverfahren: Ver- und Entschlüsselung mit gleichem Schlüssel

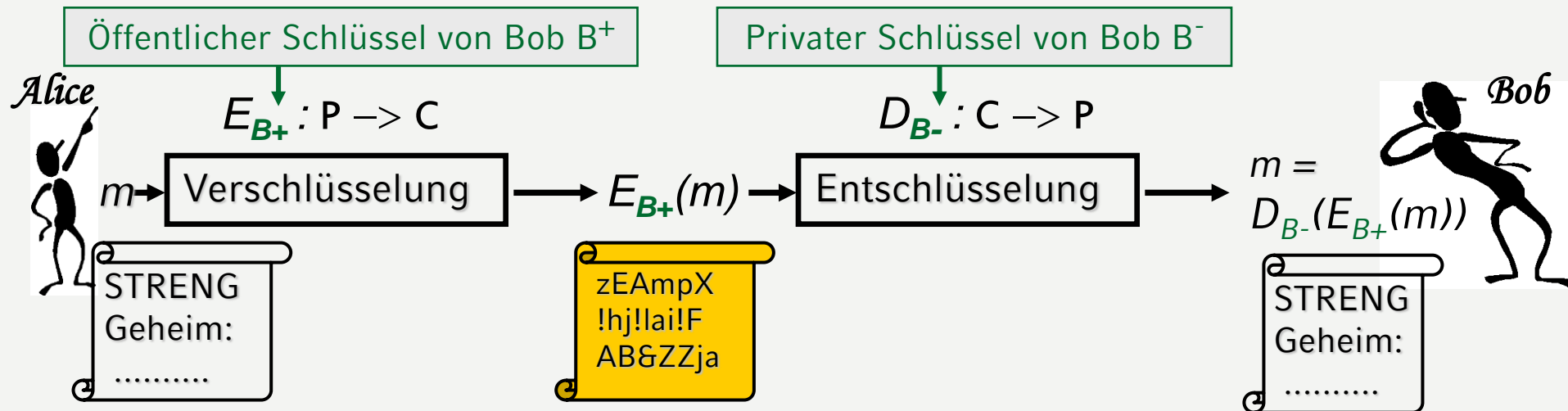
→ Schlüssel muss vorher ausgetauscht werden!



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

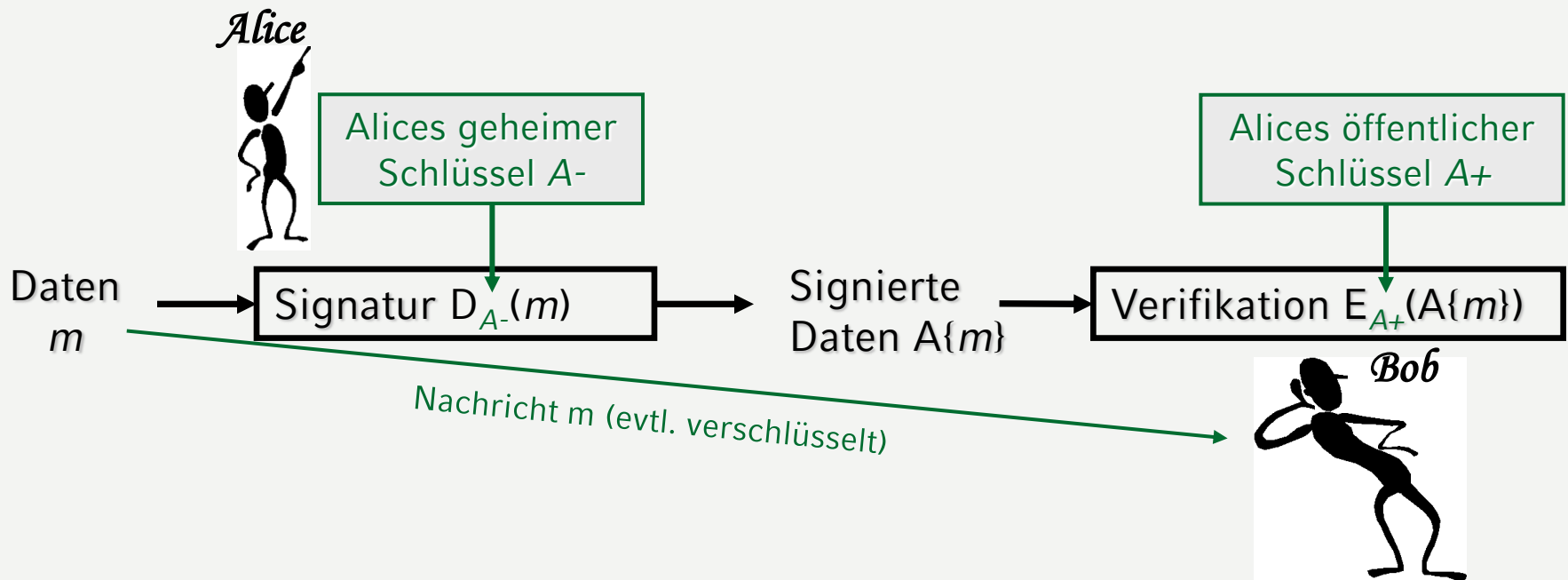
- persönlichem, geheim zu haltendem Schlüssel (**private key**)
- und öffentlich bekannt zu gebendem Schlüssel (**public key**)

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:

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

Alice „signiert“ Nachricht m mit ihrem privaten Schlüssel $A\{m\} =_{\text{def}} D_{A^-}(m)$
Jeder kann die Signatur mit Alices öffentlichem Schlüssel überprüfen



Asymmetrische Verfahren sind im Vergleich zu symmetrischen sehr langsam.
Nur Fingerabdruck = **kryptographischer Hash-Wert** 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/>

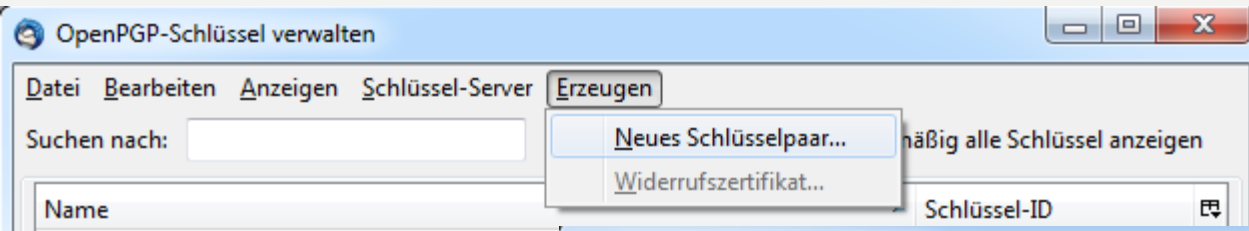
GnuPG

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

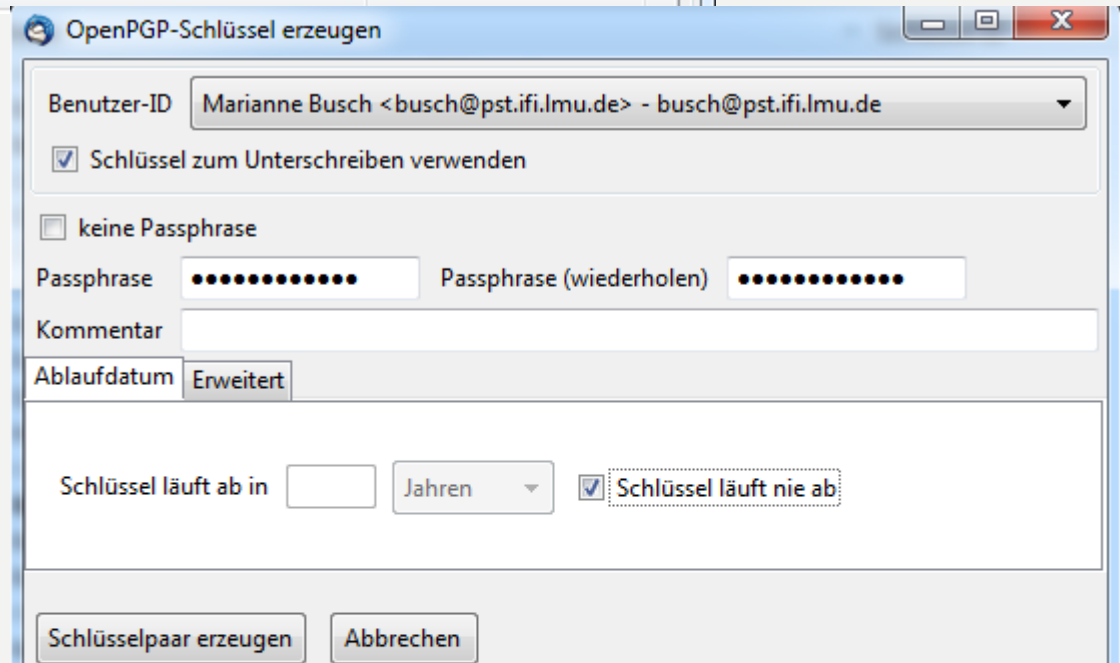
Enigmail

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

OpenPGP / Schlüssel verwalten



Neues Schlüsselpaar



Konsole zum Erzeugen eines Schlüssels

ACHTUNG: Das Erzeugen eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um das Erzeugen eines Schlüssels zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.



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

In der Praxis:

- Die Kombination signiert & verschlüsselt ist sinnvoll
- Kompletter Mail-Header bleibt unverschlüsselt (Betreff, Empfänger, Sender)
- Anhänge wenn gewünscht vorher extra verschlüsseln

Verfassen: Test

Datei
 Bearbeiten
 Ansicht
 Optionen
 OpenPGP
 Extras
 Hilfe

Senden
 Rechtschr.
 Anhang
 OpenPGP
 S/MIME
 Speichern

Von: Marianne Busch <Marianne.Busch@lmu.de>
 An: adele@gnupp.de
 Betreff: Test

Nachricht unterschreiben Strg+Umschalt+S
 Nachricht verschlüsseln Strg+Umschalt+E
 PGP/MIME verwenden
 Empfängerregeln ignorieren

Hallo Adele,
Dies ist ein Test.
Viele Grüße,
Marianne

OpenPGP-Eingabe

Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein

.....

Erst nach 5 Minuten Untätigkeit vergessen

OK Abbrechen



-----BEGIN PGP MESSAGE-----

Charset: ISO-8859-15

Version: GnuPG v1.4.11 (MingW32)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org/>

hQE0AysxYodivb/UEAP+NdUnWjenTg1VutPRVJjPP45UiZbA4A3L5ZBKLqwLEsHE
rVSgF/1nwETqr4K65VuRfx2yQ3JOdCL1UD6y4EiNkrqtP66zwHJWselx1EayycYc
kxpBfHkdr33rTM1bDEirF7js1G5qUyl9DdfWr/38ZqAxx0/EI803cH0t462eVvYD
/AIGMEDR7L+eAh540Kc6fpxWSIjgQaBAVRnQ2WcBcFXjd9gMgAWIKisHgjZ+KWg
5YmXTGj4Y41s9a/JQa90MCU/vfTkpvYgQFyAWR2Zor8Kn5umnEuEfPdvX8fAjyyl
xThEAaGwdlnKj5kCXIABOMafseGMdoLa81oo66aUmcy9hQIOA2gn3nApyXd4EAga
gegYZhZnHMJyNe/pqCVszFfQ02heiDpqxDpn3aOGOkWPQKMWRnH0wWKRy/lo9GZ
3mYFJzy/SgI9bflSeJg/Ehr+NMcur86mHNHUSksS9AIYL3fwoCMhAFyI9LFUIT9r
Cyg8sXgZ/uyzlsA0+l1fVouGk52Vt4/MwAjA0DZhhC7Pvyd6cUq9FIMGPzpkWDH0
DAmn7mEnv7H41wBaH8JFp+0DVaPk5Ect8w+zWtg9yqox2xyhzM7E7Ap7e5sCbOqz
KDRPMVOFZOMkjkU4DIMPk0IOri1qpAhTty0M3QGeeDAOyngN3fdNNZA7DHDpV1Kk
y6HRFiI9Yn3g8mhL87PADwgAlkN1JFrHJmTQzra89yXjJaY0uzHG6fjP5oHTRloI
4ixFRKbvXQ6t2ZxzRUUogd0QClzxi3gNfdj8K9Hi5btnusL9dEWXpHVOBiVrkXqe
2cSUwDxTBMjTrGmTTNdGtxb0xOKgQl1dxNRTW8ekqWyW12Mm0UWfNj2ki5sbLbh
G7eKigx3WPzbm3q/SBJ52mJw3PrsIpcsBmUCHk6Uy7abKrKVqFW6v/aiGPxZus8P
HoIDU8yxm/W3Gw12VGCS7ZYib0gxb8fLJDrG9E8fUOP1L5v30ynGpyOC0dm07vd6
XJI+Lepe953jC6Xyo4FkAnddAL++H0oAdk3weLdtND/ITtLABgE5djN4Rp2ZiVrq
bVdXq9z1LXXBuRjzL7mWIUEg4031IdHYvAdstrGmppJ2oJMrV4qMshVMaT51JxFR
INs+zvuH7Y/n0FokZEvk39oPFLUnlyXWjFWLkPou7EjN+6ORUhePAczN/Q4sLB2V
eX3XrU4gQwjXB4dYSrcGgVelRf8AME36+mgbNTjeQ03SL/APaOX2xScLbQmPy+Rg
cAo/fHIGSj4EcolRE547qE007FSxhFQ+7pP6OMGNg6AJypvAI010/7+23Q==
=WE+W

-----END PGP MESSAGE-----



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

Beispiele für Signaturen von Schlüsseln (gegen Ausweiskontrolle)

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

Search results for 'mariannebusch'

Type	bits/keyID	cr. time	exp time	key expir
------	------------	----------	----------	-----------

pub	1024D/ 31D13E63			
-----	---------------------------------	--	--	--

uid [Marianne Busch](#) <MarianneBusch@gmx.de>

sig sig3 [31D13E63](#) 2007-07-29 _____ 2012-07-27 [[selfsig](#)]

sig sig3 [DAFFB000](#) 2008-01-25 2012-07-27 _____ <pgpCA@ct.heise.de>

sig exp [65D0FD58](#) 2010-05-11 2011-05-12 _____ [CA Cert Signing Authority \(Root CA\)](#) <pgp@cacert.org>

Policy URL: <http://www.cacert.org/cps.php>

sig sig [65D0FD58](#) 2012-02-27 2013-02-27 _____ [CA Cert Signing Authority \(Root CA\)](#) <pgp@cacert.org>

Policy URL: <http://www.cacert.org/cps.php>

```
Public Key Server -- Get ``0x4b52cd1c31d13e63 ''
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: SKS 1.1.0
```

```
mQGIBeAs++sRbADByjZvL1RZy8Obb6FiJGqfKjMupYwav
wxS0uAj3qE2rONoEUy28eG3HYhXy9ul6q0DOBEIP/rRL4
1+9geAU93Fh/qv1QGdsnLgC0hUA3sQPp6clxH5fMXwCg
/jq+33lnwwTrOWzK6bWAFj6tK+iraXmQx4C2bnEZaQ5jN
O6PeEjmbuoZfoFgvUbct20MvTXBc7SqsycX4l+ehrHMD
CbfFtKxuihXxH1ZkNymZbw53j4IBA/9juQeVtsKW0miXr+
...
```



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)




Firefox Plugin Firesheep

<http://www.youtube.com/watch?v=eUyrMVkRTII>

- Abfangen von unverschlüsselten Cookies
- Ausnutzen zum Einloggen
- in unverschlüsselten (WLAN-) Netzen
- in unverschlüsselten HTTP-Sitzungen
z.B. Facebook, Twitter, youtube, myspace,...











Beispiel:
Facebook-Anmeldung
Facebook „durchstöbern“

 Anmelden | Facebook



facebook.com

https://www.facebook.com/login.php

-  Allgemein
-  **Sicherheit**
-  Benachrichtigungen
-  Abonnenten
-  Anwendungen
-  Handy
-  Zahlungen
-  Facebook-Werbeanzeigen

Sicherheitseinstellungen

Sicherheitsfrage

Sicheres Durchstöbern



Facebook mithilfe des sicheren Durchstöberns (https) verwenden, wenn möglich

Änderungen speichern

Abbrechen

**Generelle Lösung durch Browser-Plugin,
dass automatisch auf sichere Seiten 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)
- Beim Surfen möglichst sichere
https-Verbindungen verwenden



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



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 Software

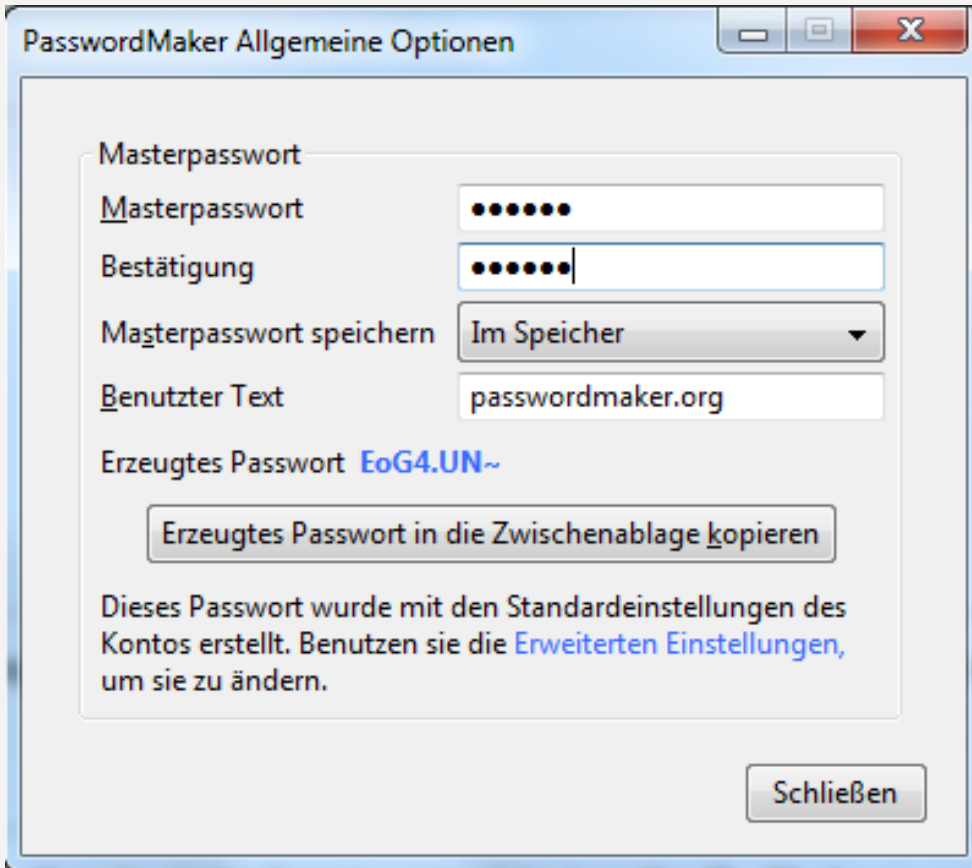
Sätze bilden: „Karl kauft über 7 Kilo frisches Obst und kocht daraus viele Gläser leckere Marmelade“

→ Kk7Kf&ukdvGIM

Software: z.B. PasswordMaker <http://passwordmaker.org/>

PasswordMaker <http://passwordmaker.org/>

Erzeugt aus Masterpasswort + URL (beliebigem Text) ein Kennwort



Masterpasswort

Masterpasswort

Bestätigung

Masterpasswort speichern

Benutzer Text

Erzeugtes Passwort **EoG4.UN~**

Dieses Passwort wurde mit den Standardeinstellungen des Kontos erstellt. Benutzen sie die [Erweiterten Einstellungen](#), um sie zu ändern.

- 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

Personal Settings

Security



[Changing your password](#)

[Recovering your password](#)

[Using 2-step verification](#)

[Authorizing applications & sites](#)

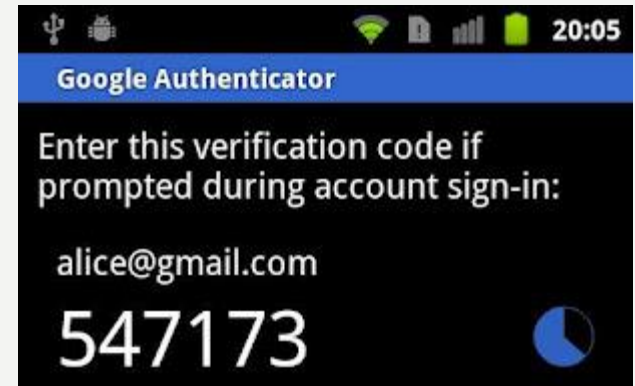
Dashboard

[View data stored with this account](#)



Verwenden

- Am Smartphone Nummer ablesen
- In Web-Formular eingeben



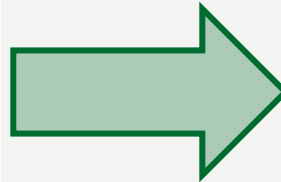
Sign in Google

Email

Password

Stay signed in

[Can't access your account?](#)



Google accounts

Enter verification code

To verify your identity on this computer, enter the verification code generated by your mobile application.

Enter code:

[Other ways to get a verification code »](#)



Verwenden

- Am Smartphone Nummer ablesen (oder von Liste / Anrufservice)
- In Web-Formular eingeben

Anwendungsspezifische Passwörter:

Schritt 1 von 2: Neues anwendungsspezifisches Passwort generieren

Geben Sie einen Namen ein, der auf die Funktion dieser Anwendung hinweist:

Name:

Beispiele: "Christians Android", "Google Mail auf meinem iPhone", "Google Talk", "Outlook - zu Hause", "Thunderbird"

Ihre anwendungsspezifischen Passwörter	Erstellungsdatum	Datum der letzten Verwendung	
Thunderbird Mail	18.02.2011	20.02.2012	[Aufheben]
Thunderbird Mail outgoing	18.02.2011	22.02.2012	[Aufheben]
PidginPC	18.02.2011	22.02.2012	[Aufheben]



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“*

Diese Nummer wird dann sofort im Browser eingegeben.



Wer hat Zugriff?

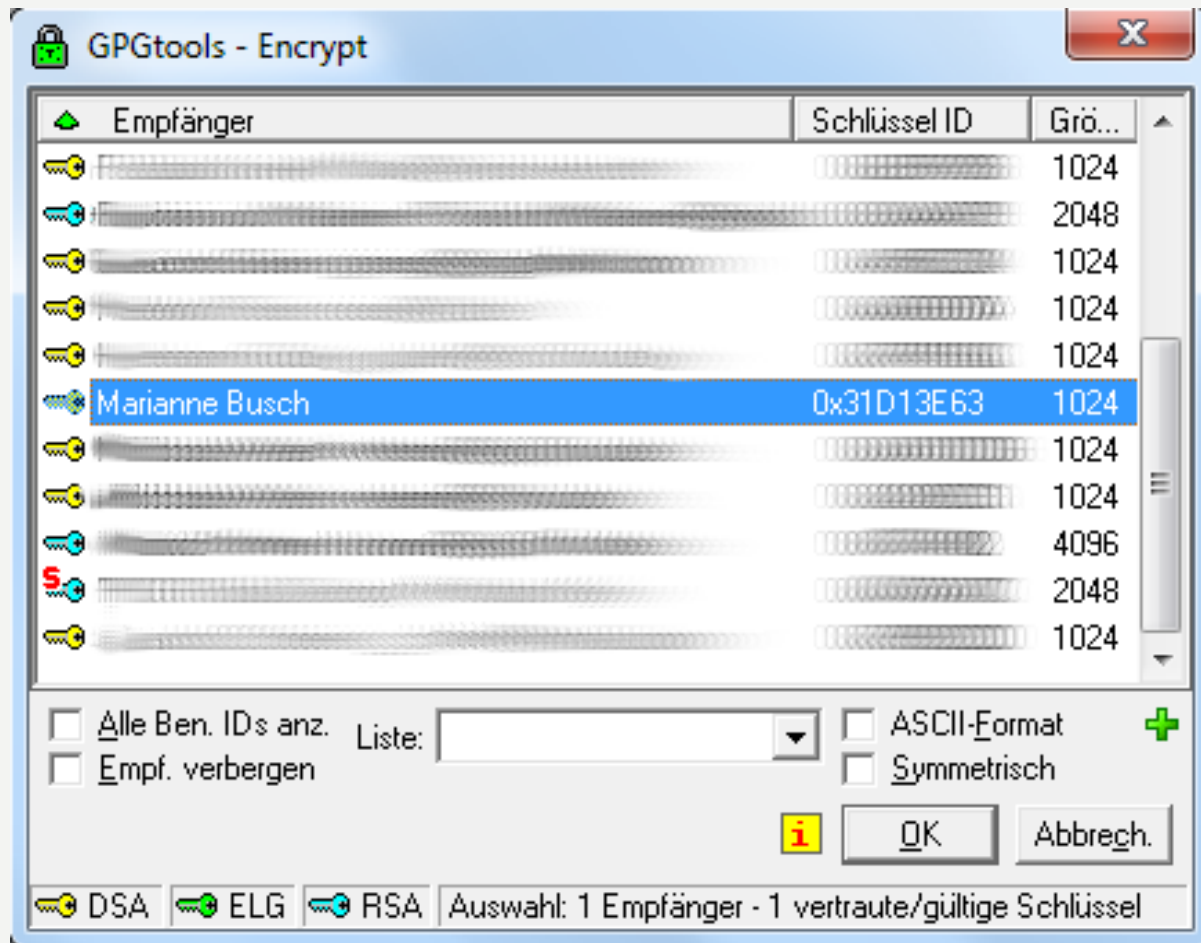
- Freunde?
- Kollegen?
- Spaßvögel?
- Trojaner?
- Diebe?

Auf was?

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

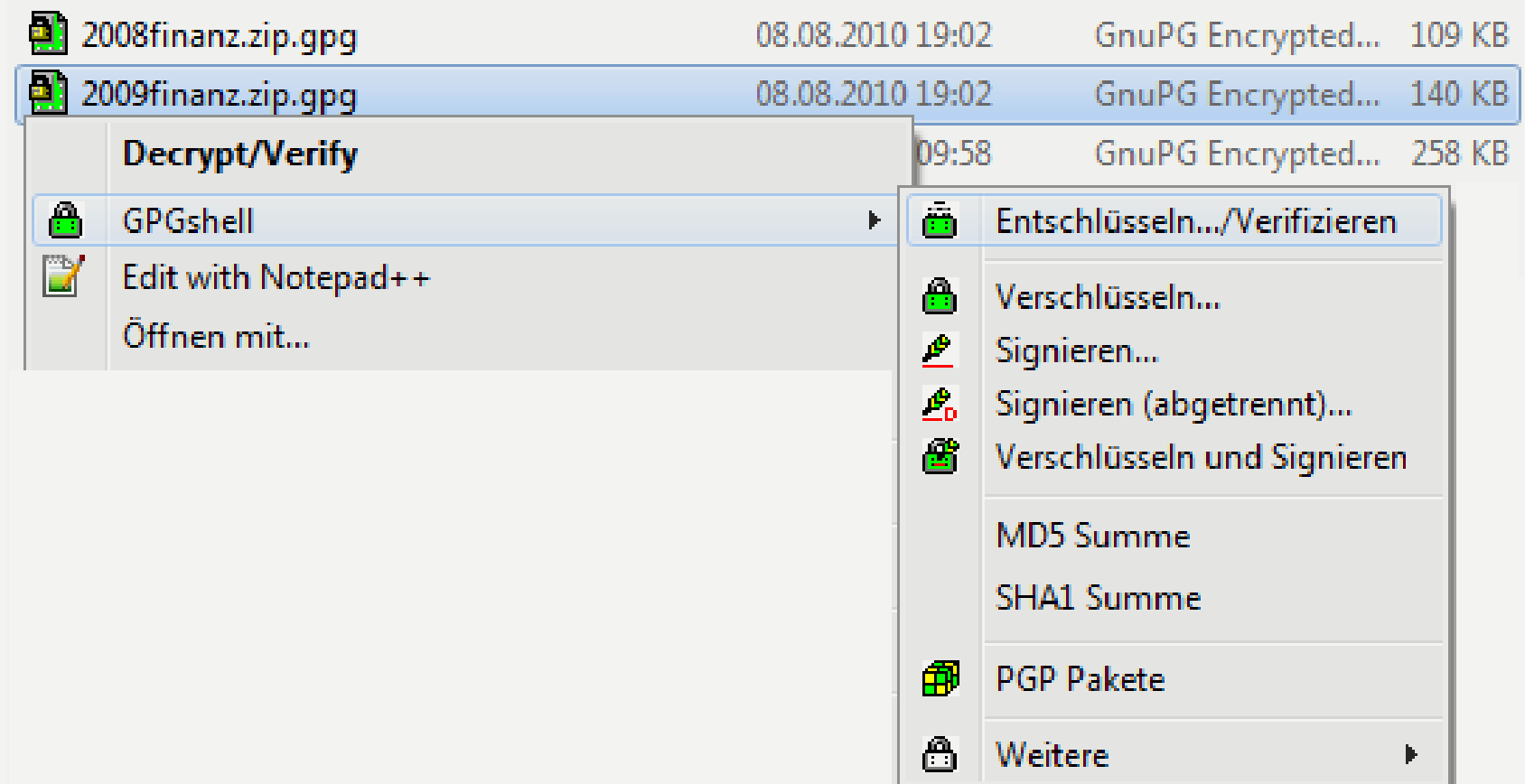
Verschlüsseln einzelner Dateien z.B. mit gpg4win

<http://gpg4win.de>



Entschlüsseln einzelner Dateien z.B. mit gpg4win

<http://gpg4win.de>



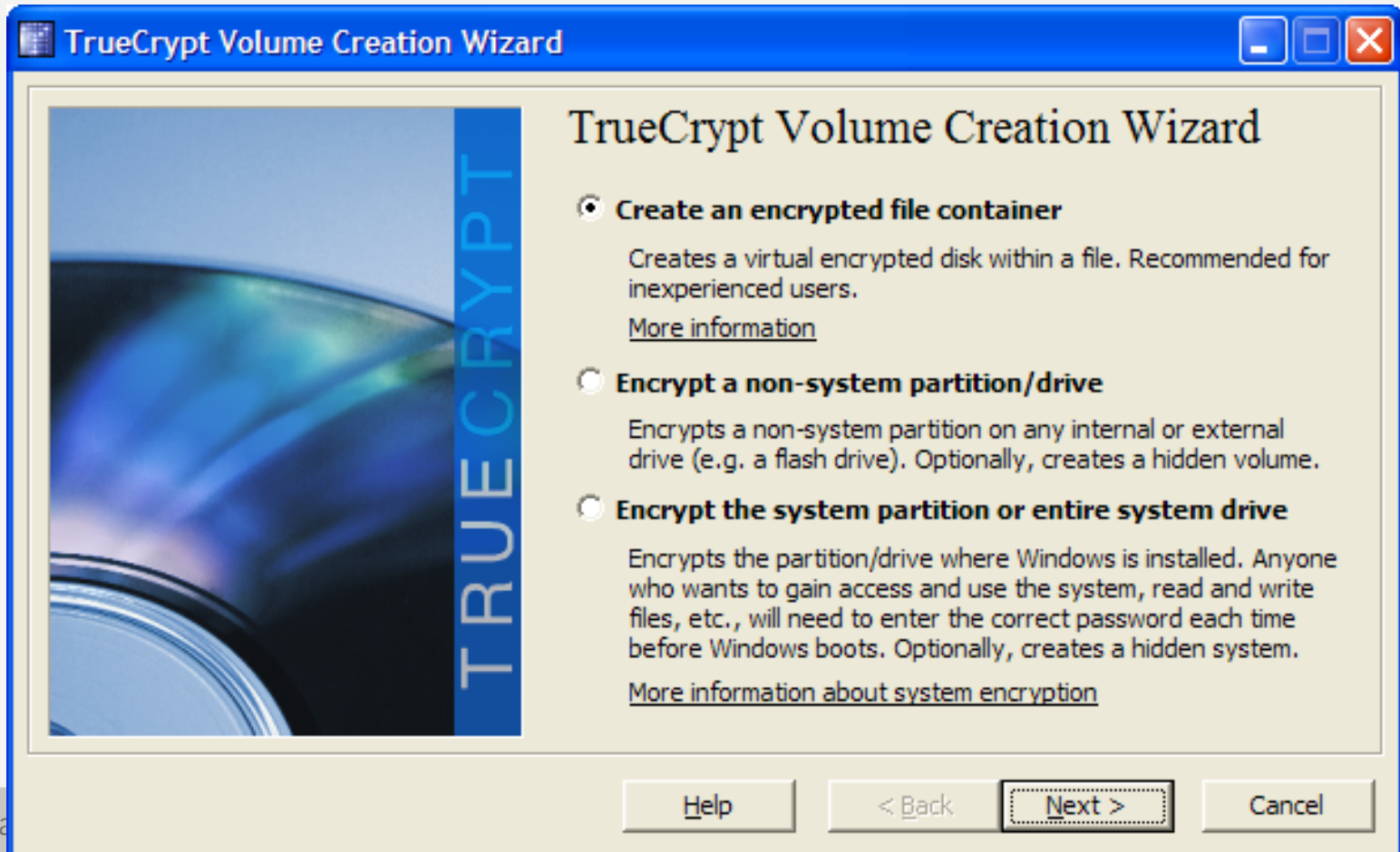
The screenshot shows a file explorer window with three encrypted files:

File Name	Date	Time	Encryption Method	Size
2008finanz.zip.gpg	08.08.2010	19:02	GnuPG Encrypted...	109 KB
2009finanz.zip.gpg	08.08.2010	19:02	GnuPG Encrypted...	140 KB
		09:58	GnuPG Encrypted...	258 KB

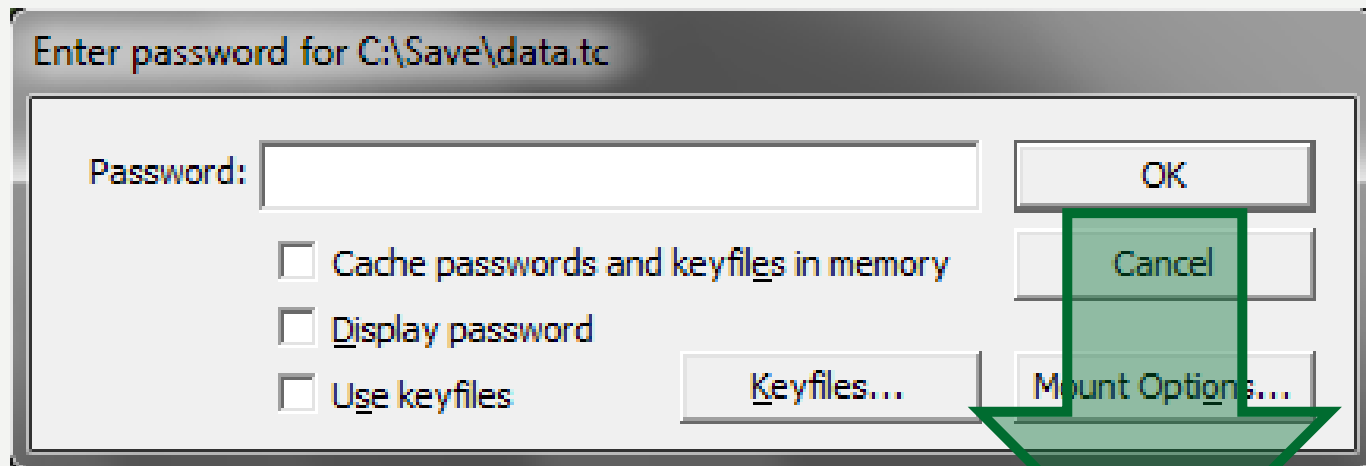
A context menu is open over the selected file, showing the following options:

- Decrypt/Verify
- GPGshell
- Edit with Notepad++
- Öffnen mit...
- Entschlüsseln.../Verifizieren
- Verschlüsseln...
- Signieren...
- Signieren (abgetrennt)...
- Verschlüsseln und Signieren
- MD5 Summe
- SHA1 Summe
- PGP Pakete
- Weitere

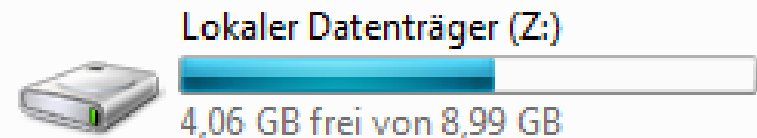
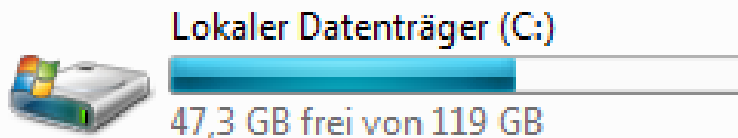
Verschlüsseln einzelner Dateien z.B. mit OpenPGP
Verschlüsseln ganzer Partitionen z.B. mit TrueCrypt
<http://www.truecrypt.org/>



Verschlüsseln einzelner Dateien z.B. mit OpenPGP
Verschlüsseln ganzer Partitionen z.B. mit TrueCrypt
<http://www.truecrypt.org/>



▲ Festplatten (2)





Kennwörter eingeben ist lästig



Smartphones werden leicht geklaut



Synchronisieren über das Web ist bequem



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



Apps ausprobieren ist sehr praktisch



Sicherheitsrisiken (trotz Virens Scanner)



„Android-Lücken ermöglichen die heimliche Installation von Apps“

<http://heise.de/-1134661> (11.2010)

„Forscher demonstriert Schwächen des Android-Rechtesystems“

<http://heise.de/-1399337> (12.2011)

„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

Android ist hier nur ein Beispiel auch für andere Smartphone Betriebssysteme findet man Lücken



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**



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

➔ Heutzutage: Spear-Phishing

s. Technology Review von Nov 2011

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



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

I-Frame für Like-Button

Cookie und Referer werden an Facebook gesendet

- Facebook 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:

z.B. <https://addons.mozilla.org/de/firefox/addon/facebook-blocker/>

<http://heise.de/-1230906>

<http://heise.de/-1333879>



↓ 1. Klick: aktivieren



↓ 2. Klick: empfehlen





Fragen?

Sicherheitslücken gibt es täglich neue ...
... Informatiker werden dringend gebraucht!