Kryptografie

Verschlüsselung für Mail & Devices

David Dorst

Anja Hirschel

PIRATEN PARTEI

Ulm (und um Ulm herum)

Übersicht

- Warum Kryptografie?
- Geschichte der Kryptografie
- Menschliches Versagen
- Verschlüsselungsverfahren
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hybride Verschlüsselung
- Zertifikate
- Tools für die Mailverschlüsselung
- Devices

Warum Kryptografie?

Laut einer Analyse von Gartner sind 57 % aller erfolgreichen Netzwerkangriffe auf einen Notebook- Diebstahl zurückzuführen.

Weniger als 40% aller Laptops sind verschlüsselt.

Vergessene Laptops im Fundamt der DB: 500 (im Jahr 2009)

Gespeicherte Bookmarks und Passwörter auf Laptops ermöglichen den Zugriff auf Mails, Firmennetzwerke usw.

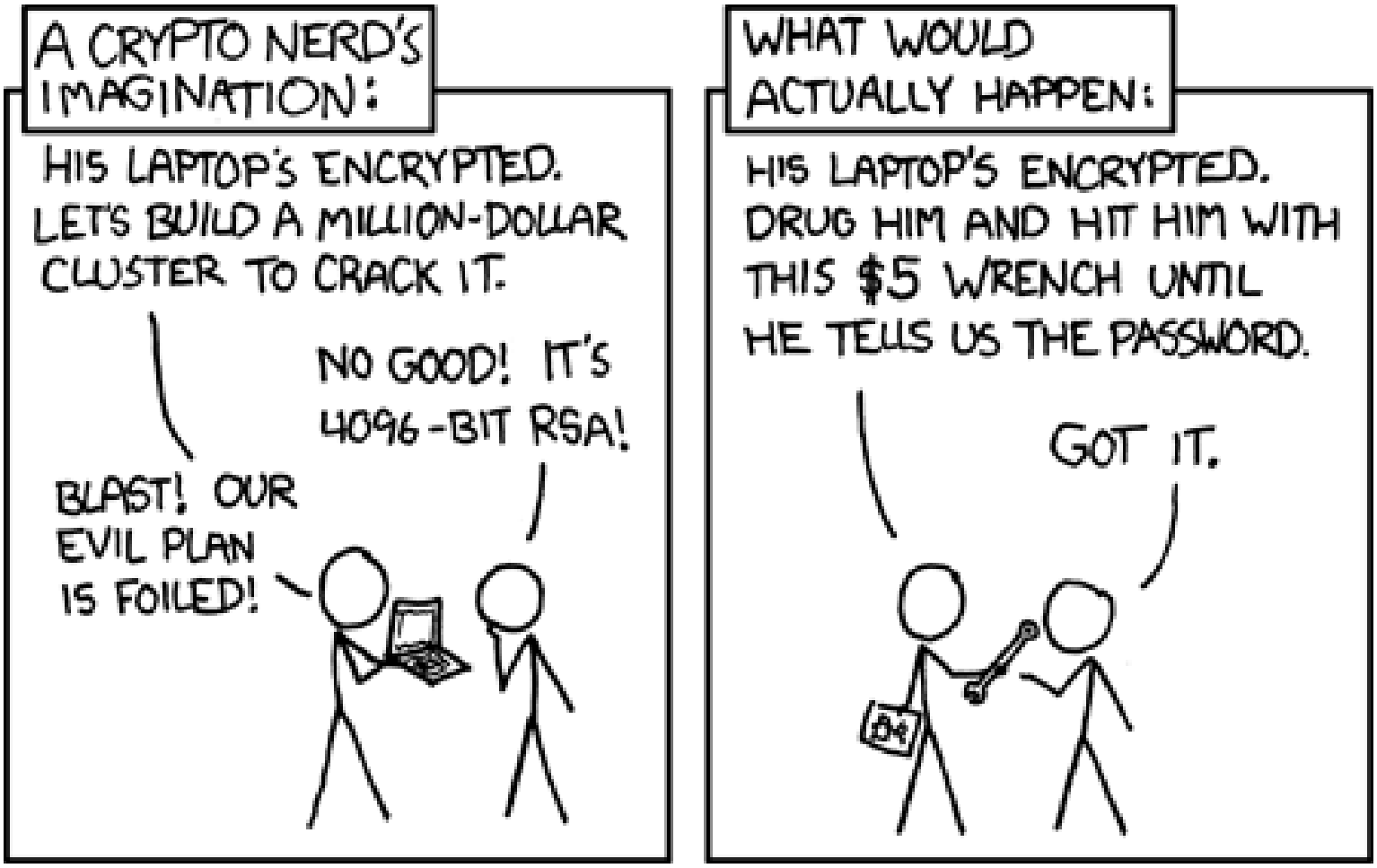
Geschichte der Kryptografie

Kryptographie bzw. **Kryptografie**

(von altgriechisch κρυπτός *kryptós* ‚verborgen, geheim' und γράφειν *gráphein* ‚schreiben') war ursprünglich die Wissenschaft der Verschlüsselung von Informationen.
Heute befasst sie sich allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind.

Quelle: http://de.wikipedia.org/wiki/Kryptographie

Menschliches Versagen

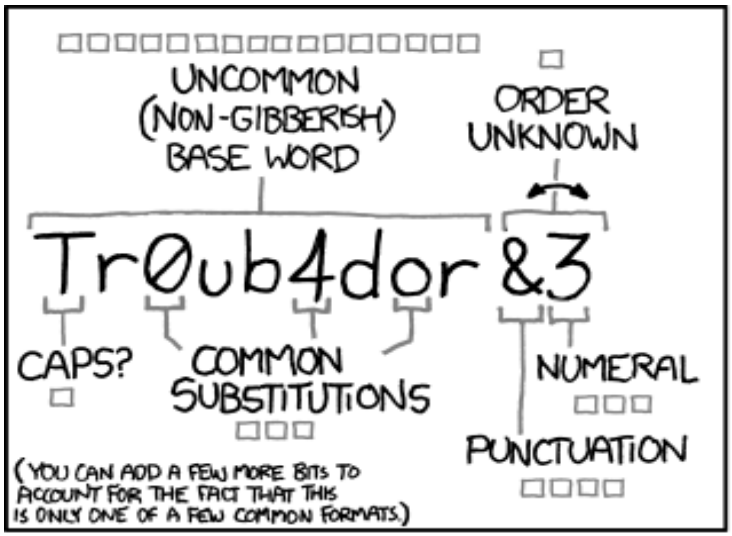


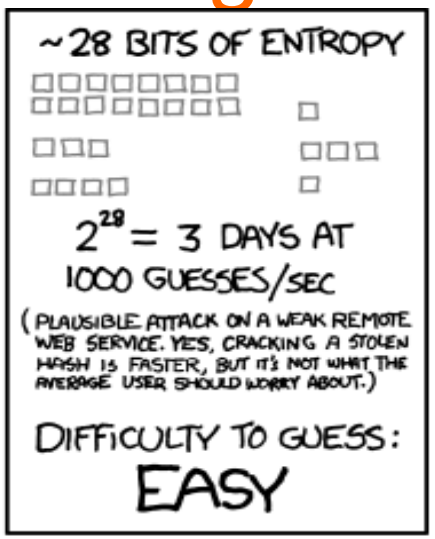
Menschliches Versagen

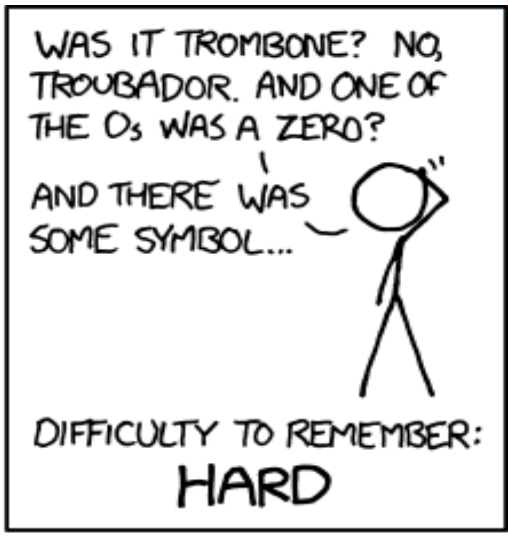
- Bewusstsein: Daten sind Macht
- Bewusstsein: Wissen birgt Gefahr
- Bewusstsein: Daten werden ständig herausgegeben
- Bewusstsein: Absichten des Gegenüber unbekannt
- Angriffsoption: Physische Gewalt
- Angriffsoption: Aushorchen ohne Gewalt

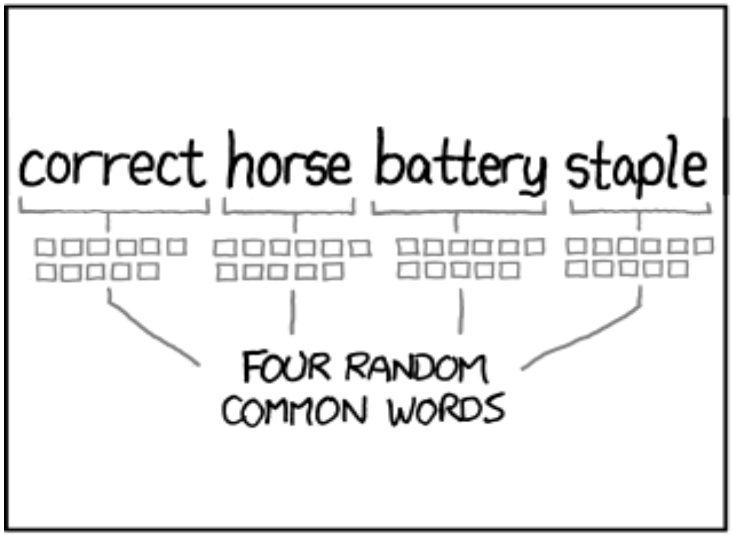
„Hi, wie geht's dir?“
„Achjo, kann nicht klagen.“
„Wie heisst du? Kenne ich dich nicht?“
„Max Mustermann, aber nein wir sehen uns heute zum ersten mal?!“
„Max Mustermann? Du bist doch am 3.5.1989 geboren, dein Vater ist doch der Klaus?“
„Nein, nein, ich bin am 2.4.1980 geboren und mein Vater heisst Martin.“
„Oh, tut mir leid, eine Verwechslung, 'tschuldige“ - Und vielen Dank für Zugriff auf deine Mails, Ebay, Paypal... .

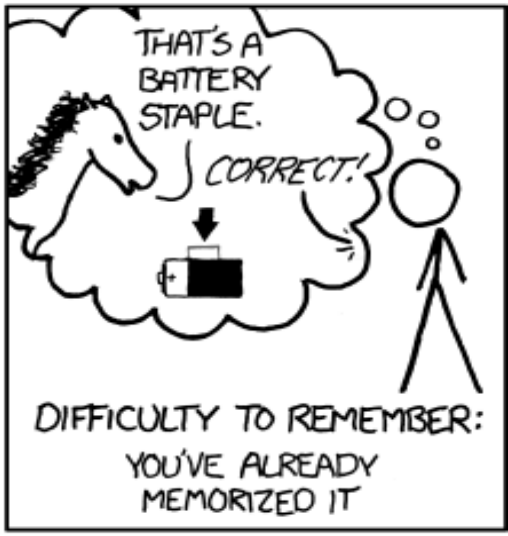
Menschliches Versagen











THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Menschliches Versagen

Hierzu aus dem Spiegel, 26.01.2011
„Spionage in linker Szene
Deutsche Behörden forderten Briten-Spitzel an

Berlin - Mark Kennedy ist abgetaucht. Der Brite lebe in den USA, heißt es, genaueres weiß man nicht. Es gibt viele, die hinter ihm her sind. Denn kürzlich flog auf, dass er als verdeckter Ermittler von Scotland Yard unter dem Alias Mark Stone jahrelang Europas linke Szene ausspionierte. Ein spektakulärer Fall.

[…]

Der Einsatz des Briten ist heikel. Noch immer steht der Vorwurf im Raum, Kennedy habe als "Agent Provocateur" Aktivisten bei Protesten gegen die Polizei aufgewiegelt. Dem SPIEGEL berichteten zwei ehemalige Weggefährten Kennedys von entsprechenden Vorfällen. Auch führte der britische Undercover-Cop über mehrere Jahre eine Fernbeziehung mit einer Frau, die damals in Berlin lebte.

Menschliches Versagen

Taktische Liebesbeziehungen, sagte Ziercke in der Sitzung, seien hierzulande nicht zulässig und widersprächen jeglichen Regeln, die in Deutschland für verdeckte Ermittler gelten würden. Was die Kontrolle der Undercover-Polizisten angehe, gebe es aber noch gewisse Defizite, räumte er nach Angaben mehrer Anwesender ein.“

Menschliches Versagen

„Ich bin doch als Ziel uninteressant“ - Ist das so?

Veranlassung kann mannigfaltig sein:

- Macht
- Information als Selbstzweck
- Abneigung/Hass/Rache
- „4 the lulz“
- uvm.

Gerne genutzt: Information über das Sexualleben

Verschlüsselungsverfahren

Möglichkeiten Texte zu verbergen:

Transposition – Umverteilen von Zeichen

Substitution – Ersetzen von Zeichen

Kodierung – Ersetzen von Buchstaben/Worten/Sätzen

Verschlüsselungsverfahren

ROT-13 (Rotation um 13 Zeichen)
(auch bekannt als Caesar Chiffre)

Alphabet (klar):
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Alphabet (geheim):
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

Wort (klar):
D A V I D

Wort (geheim):
Q N I V Q

Verschlüsselungsverfahren

Die Umkehren durch nochmalige Anwendung

Rot13(DAVID) → QNIVQ
Rot13(QNIVQ) → DAVID

Monoalphabetisch – 1 Klartextalphabet – 1 Geheimtextalphabet

Verschlüsselungsverfahren

Geschichtlich, Verfahren:

Rot13 (Caesar) – ca. 50 v. Christus

Vigenère-Verschlüsselung – ca. 16. Jhdt.

Historische Anwendung:

Enigma (2. WK)

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung dient ein einziger Schlüssel
sowohl zum Ver- als auch zum Entschlüsseln

<u>Vorteil:</u>

Sehr einfach und schnell

<u>Nachteil:</u>

Der Schlüssel muss sicher übermittelt werden

Symmetrische Verschlüsselung

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish

Asymmetrische Verschlüsselung

Ein Schlüsselpaar aus Public Key zum Verschlüsseln und Private Key zum Entschlüsseln wird erzeugt.

Vorteil:

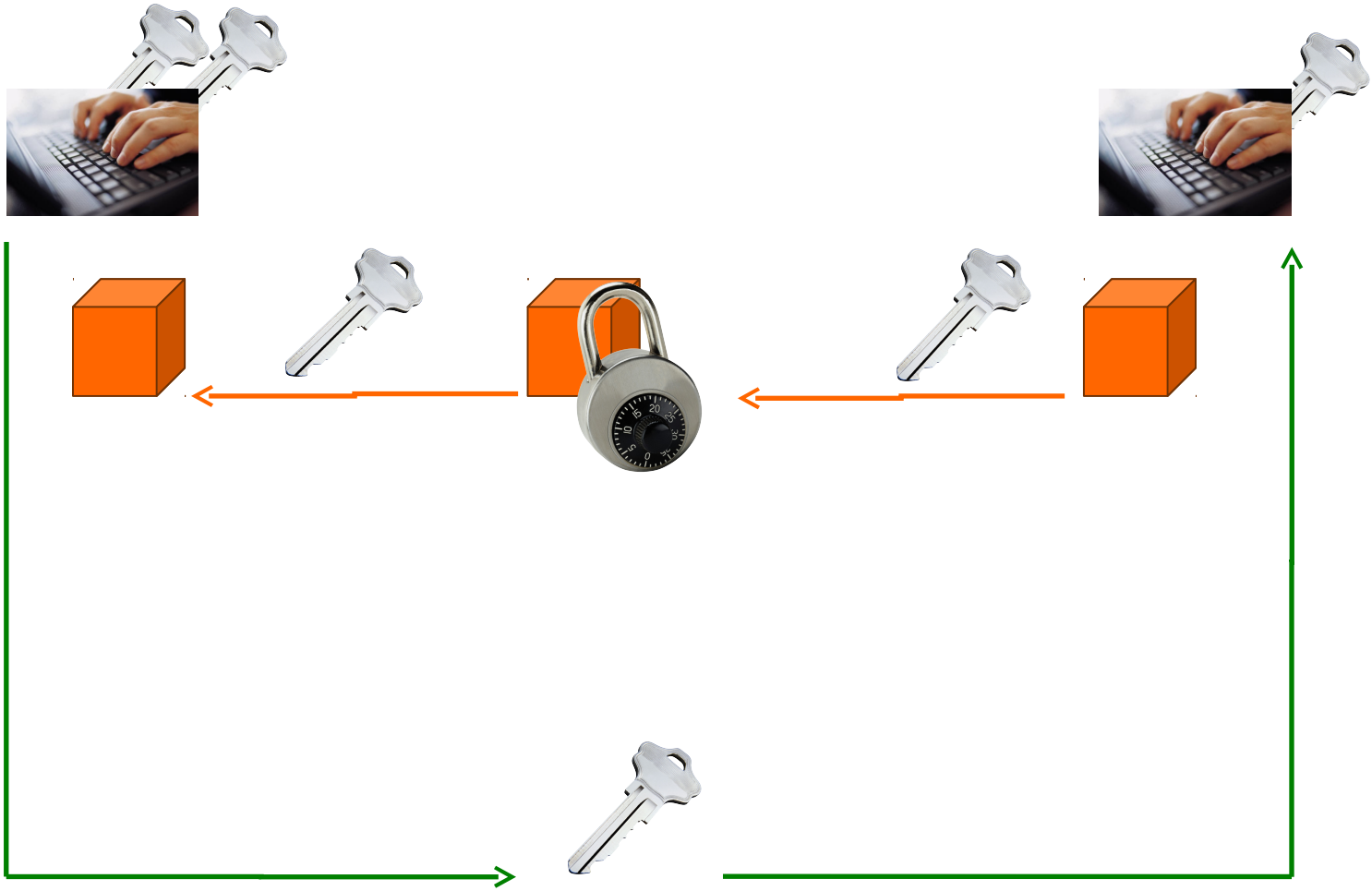
Der öffentliche Schlüssel ist frei verteilbar

Nachteil:

Aufwendigeres Verfahren z.B. Notwendigkeit von Schlüsselservern

Zertifikate um öffentlichen Schlüssel zuordnen zu können

Asymmetrische Verschlüsselung



Hybride Verschlüsselung

Kombination aus Symmetrischem und Asymmetrischem Verfahren

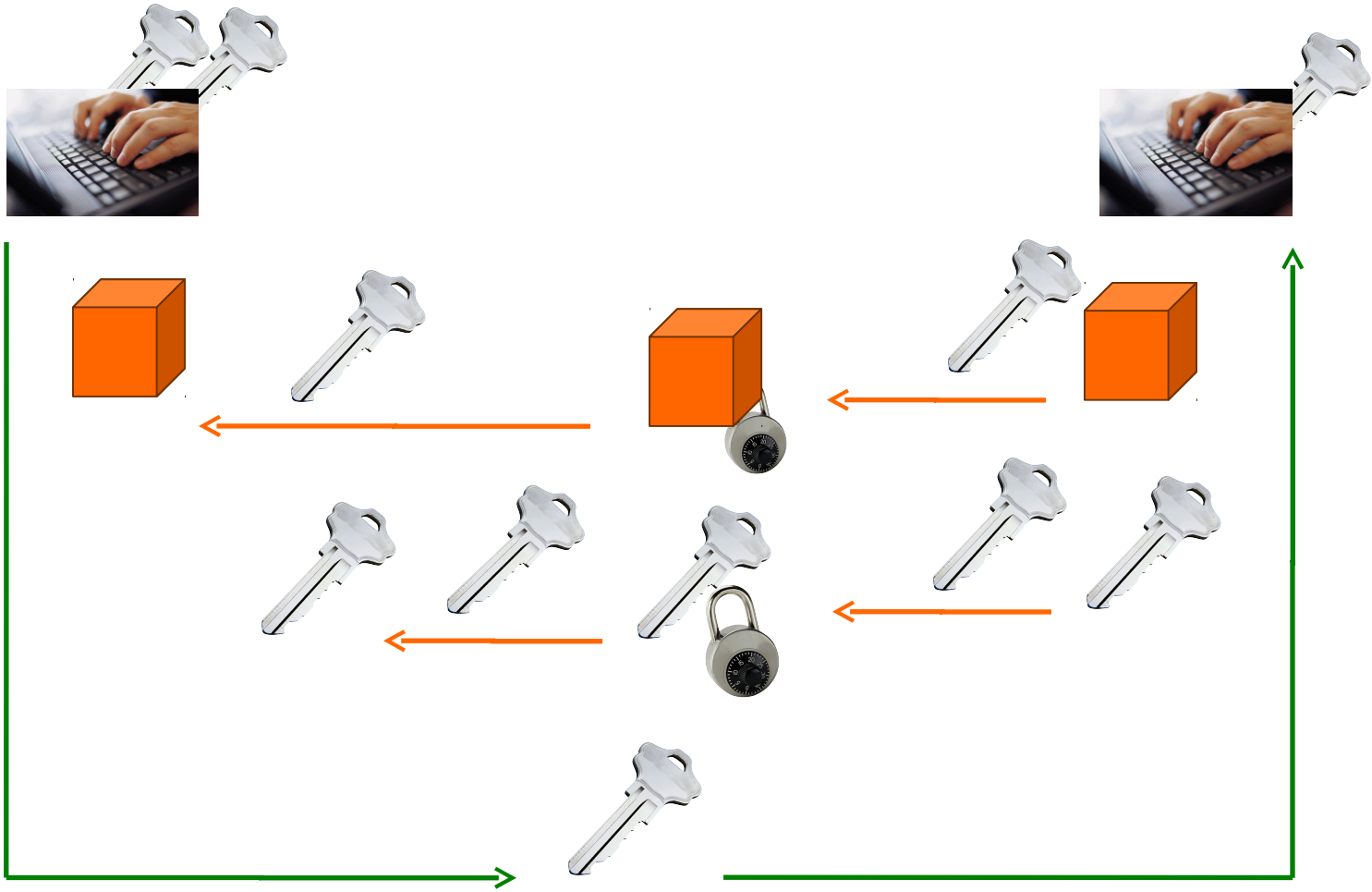
Der Session Key verschlüsselt die Daten symmetrisch, besitzt aber nur kurze Gültigkeit.

Dieser wird mit dem PublicKey des Empfängers assymetrisch verschlüsselt.

Vorteil:

Besonders für große Datenmengen sehr leistungsfähig.

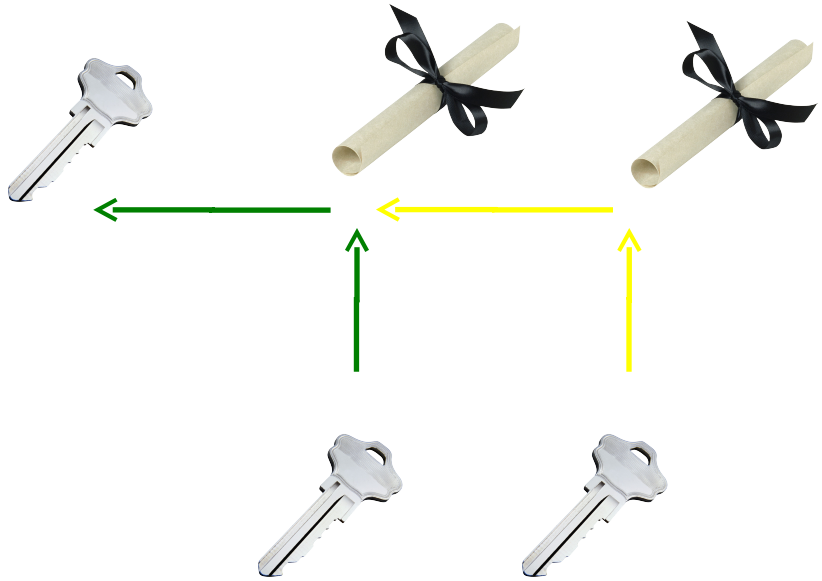
Hybride Verschlüsselung



Zertifikate

Ein Zertifikat enthält Daten, mit denen elektronische Signaturen überpüft werden können. Sie dienen dazu, die Identität z.B. des Public Keys zu bestätigen.

Diese Zertifikate selbst werden ebenfalls durch ein Zertifikat geschützt, das mit dem Publik Key des Ausstellers überprüft werden kann.



Zertifikate

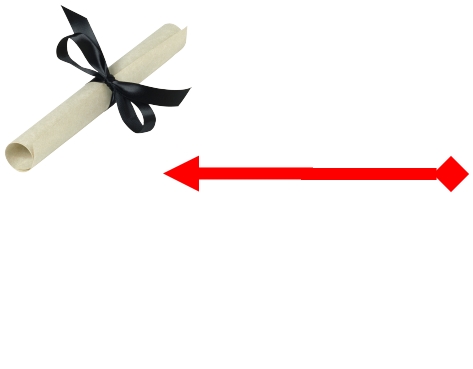
Über das gegenseitige Vertrauen von Zertifikaten lassen sich Zertifizierungspfade aufbauen. Der Echtheit des letzten Zertifikats der Kette muss vertraut werden können.

Die CA übernimmt die Zertifizierung von Zertifikatsanträgen.

Zertifizierungsstelle
Certificate Authority
(CA)

Zertifikate

Bei der Registrierungsstelle werden die Zertifikate beantragt die nach Prüfung der Identität durch die Zertifizierungstelle zertifiziert werden.



Zertifizierungsstelle
Certificate Authority
(CA)

Registrierungsstelle
Registration Authority
(RA)

Tools für Mails

Mozilla Thunderbird

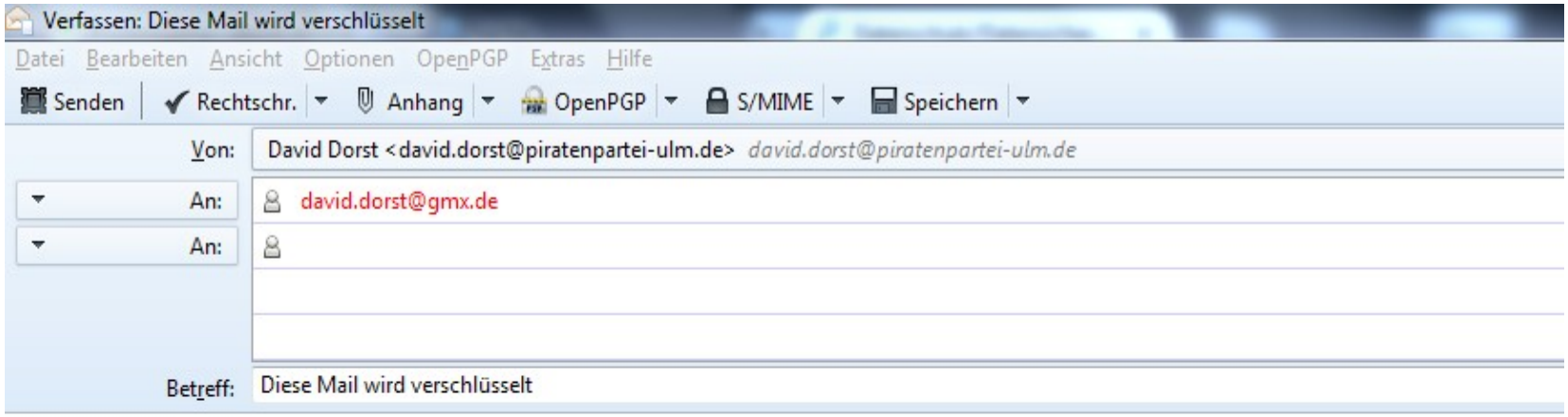
Zusätzlich die Erweiterungen:

Enigmail zum Signieren, zur Schlüsselsuche, zum Ver- und Entschlüsseln, das dann durch den GNU Privacy Guard (GnuPG) ausgeführt wird, dieser erzeugt auch die benötigten Schlüsselpaare.

HowTo:

http://wiki.piratenpartei.de/PGP/HowTo_PGP_mit_Thunderbird_unter_Windows

Verschlüsselung von Mails

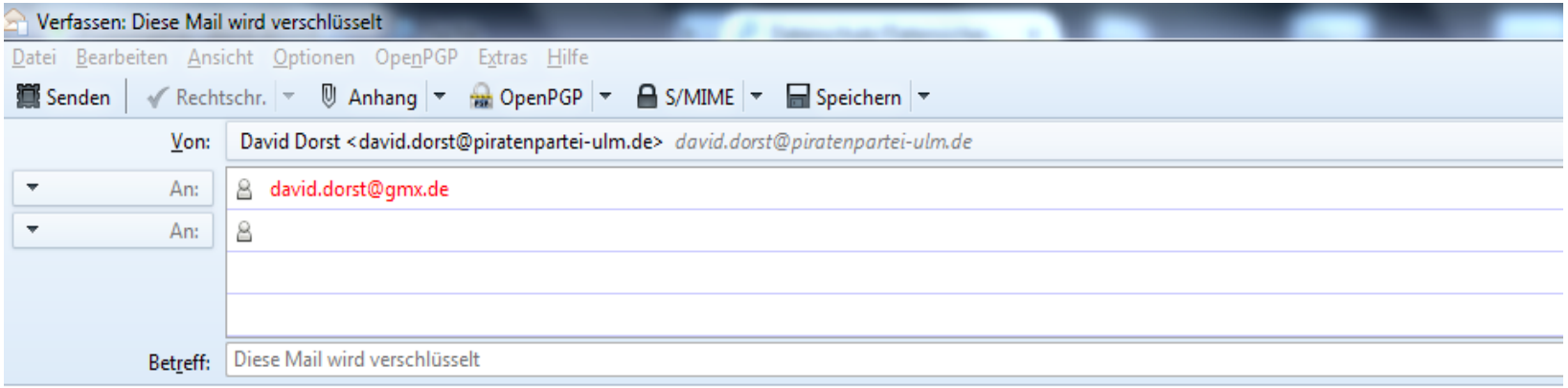


Hallo Dave,

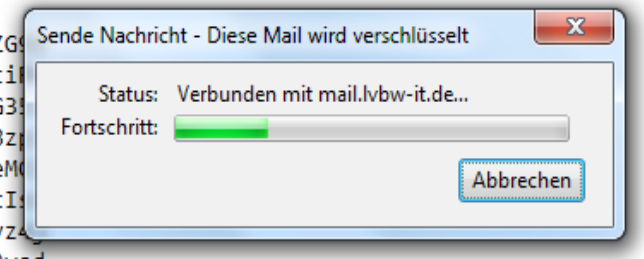
diese Mail ist nach Einsatz von OpenPGP verschlüsselt.

Gruß Dave

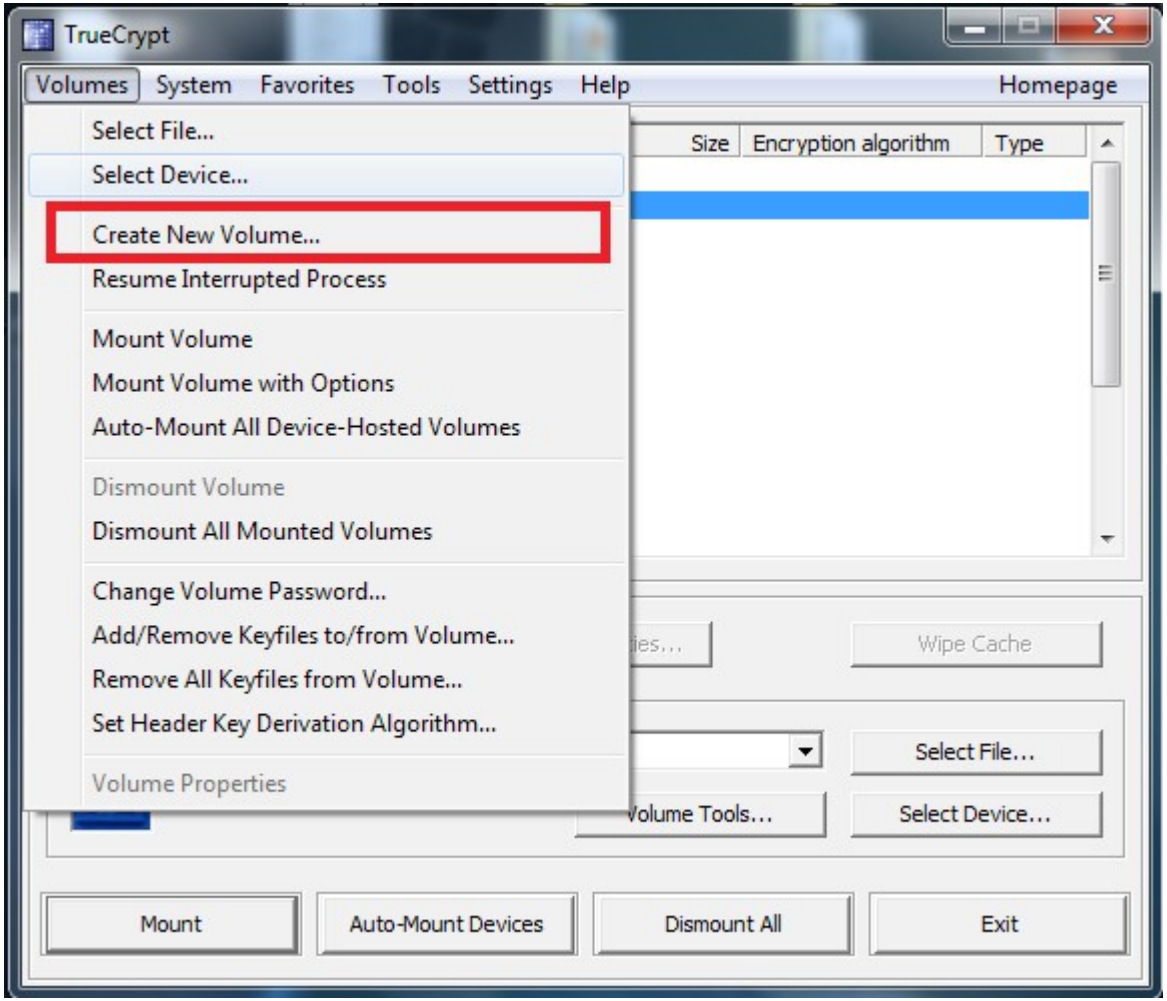
Verschlüsselung von Mails



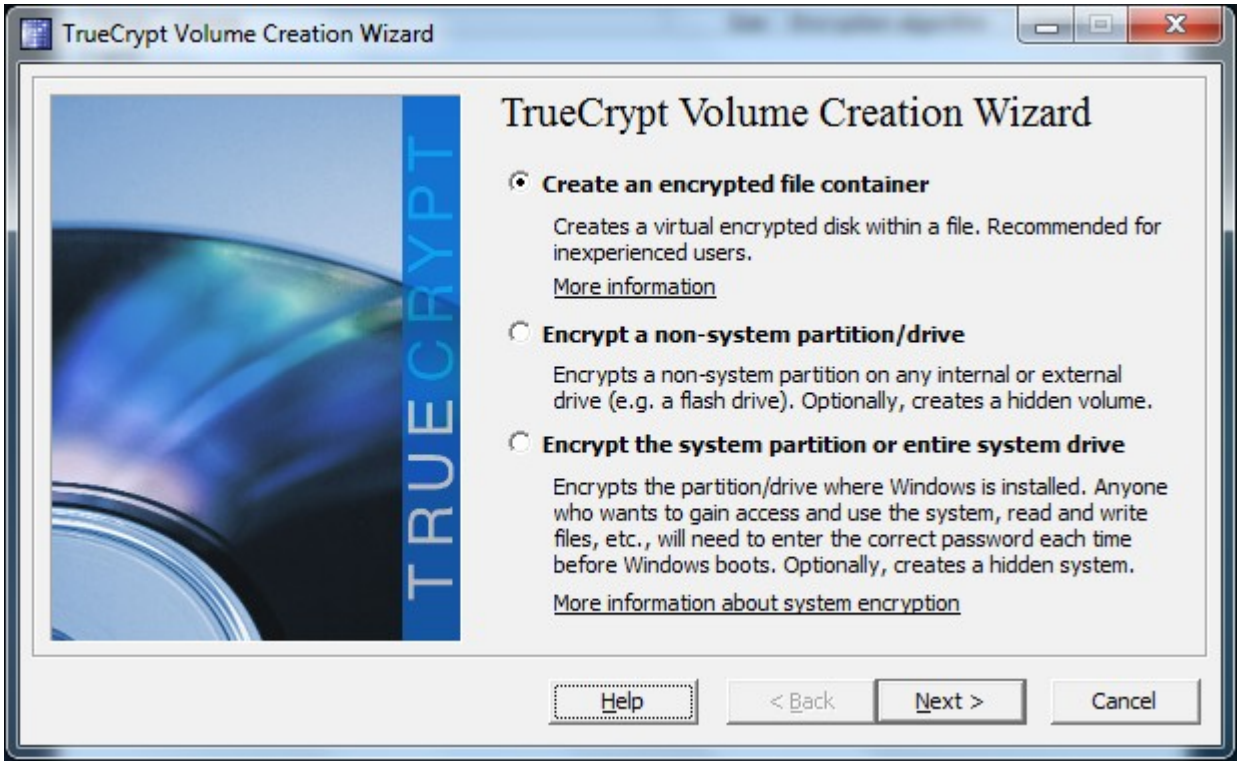

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v2.0.17 (MingW32)
Comment: Using GnuPG with undefined - http://www.enigmail.net/

hQEMA8pLbWzSRNSVAQgAi/pA/ph+A7ahmH55jBRKchZU7u2AsoiKYcjngFZRZG
Zciow7qoWafUcl63vCTwTGXue+FRUkM0dLLv5DIfUO61G3BvakvvsAr7sCPlci
/A1YjXKSFdVlwAbgUObQq4F1hTUDUMSVzl1BsFvOzGw1tz65S1UWieRxCEAJG3
10LcEwkmpHdO2Jbj4QVJAofsWjbXgreSPsD0eSfvJ2i3oNqxO2lESUHMrz0uBz
/bdzTIXrMD4khdIunh3ByCJYGoLIgfOidCjQo791oVMIUG+HNbPmVO6iQqYVeM
80vOUXUYM2ORU/ahmFarJs//R9oEuvgx912fmaOqqNLBAAHvgTzgisQhHqDRtI
SitNlpXA6EaE0t2zEH9YXir5nGT9tGg5kCxnCvMs2t/OBaO3NBiW25TIbz6xyz
OIJEc4TobJfNDuzzo62p97pTLzhthT572QG1O6mutjIIr77LXuzU0pmcnhIv2wod
fGDKHCbvKNXT1xo4kDJGcyqPy5xO7Uje4CeaZWBammQzxbpSVdXCCrpPUMqcldJ5
fwVromC7QDKNCRGYCB1QLNy76bAFSc+SWrAnzUHtbFQV1g4/X7ziX44d01cbYxtI
UiQ5PDE0A2fhse4fmEL4EFFFc2qBYxqJpPLHVgDwmjru6+PMLvxa1wo43KrgM+K/
UcOPhJxqM0M7MGILIa1EVuIjXMZXema2Z/0lMxNJ/buBaazJS9joaP2/frDfDIJ8
GPPFZ2ElYY8OwynxdEsdnpOqAMudHGD05K6Hprw1QfrtLa05sMK/SfL+Izpd9KA1
uZaEZkVyfeeaf6A7lT0oASWceeHQM1b9QvOL0exjYj9/UfktqtJ2m6oTfAFwbUYs
oH5gVBESHNECfIUMnCmtnF0CKqK6waGdYyQZ6KDfzeMFkn0At4nKJoFHc7zPWSEc
rVw=
=8gKW
-----END PGP MESSAGE-----
```



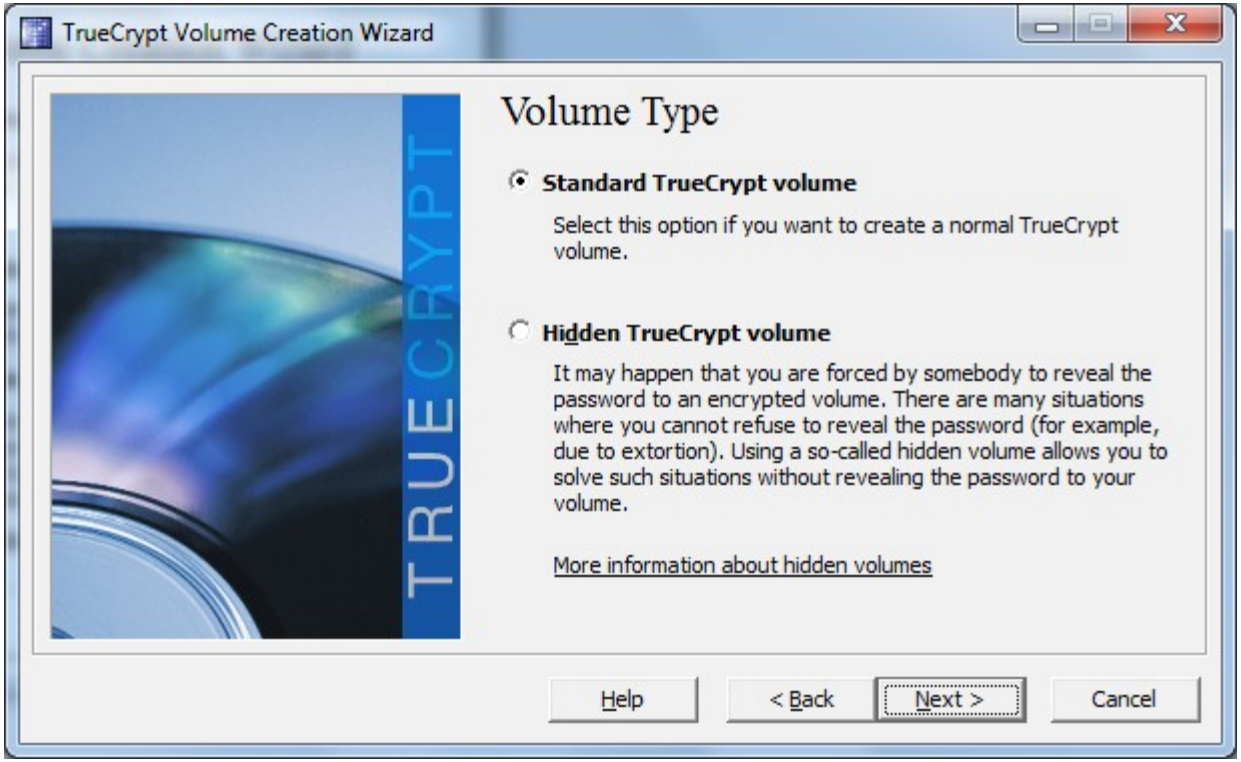
Devices


TrueCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Select File...
Select Device...
Create New Volume...
Resume Interrupted Process
Mount Volume
Mount Volume with Options
Auto-Mount All Device-Hosted Volumes
Dismount Volume
Dismount All Mounted Volumes
Change Volume Password...
Add/Remove Keyfiles to/from Volume...
Remove All Keyfiles from Volume...
Set Header Key Derivation Algorithm...
Volume Properties
Size
Encryption algorithm
Type
Wipe Cache
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Devices

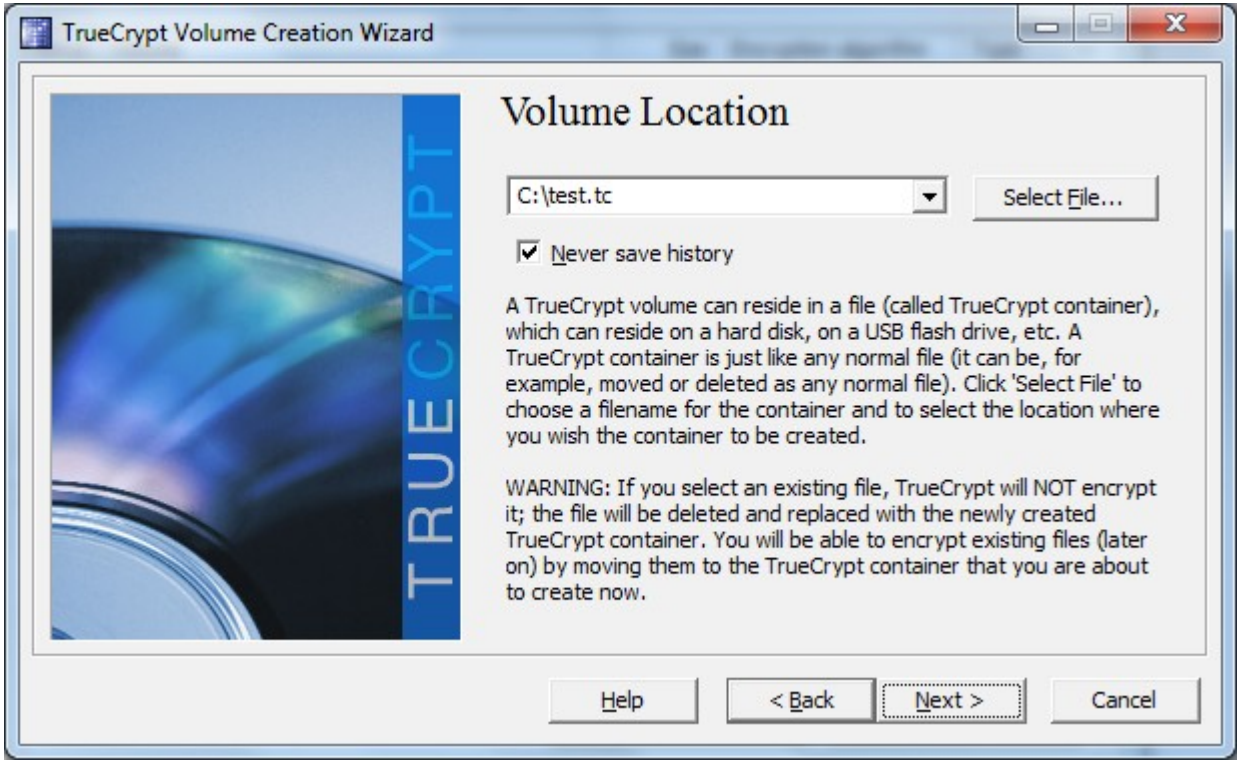

TrueCrypt Volume Creation Wizard
TRUECRYPT
TrueCrypt Volume Creation Wizard
Create an encrypted file container
Creates a virtual encrypted disk within a file. Recommended for inexperienced users.
More information
Encrypt a non-system partition/drive
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.
Encrypt the system partition or entire system drive
Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.
More information about system encryption
Help
< Back
Next >
Cancel

Devices


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
Help
< Back
Next >
Cancel

Devices

ACHTUNG: Bestehende Dateien werden überschrieben!



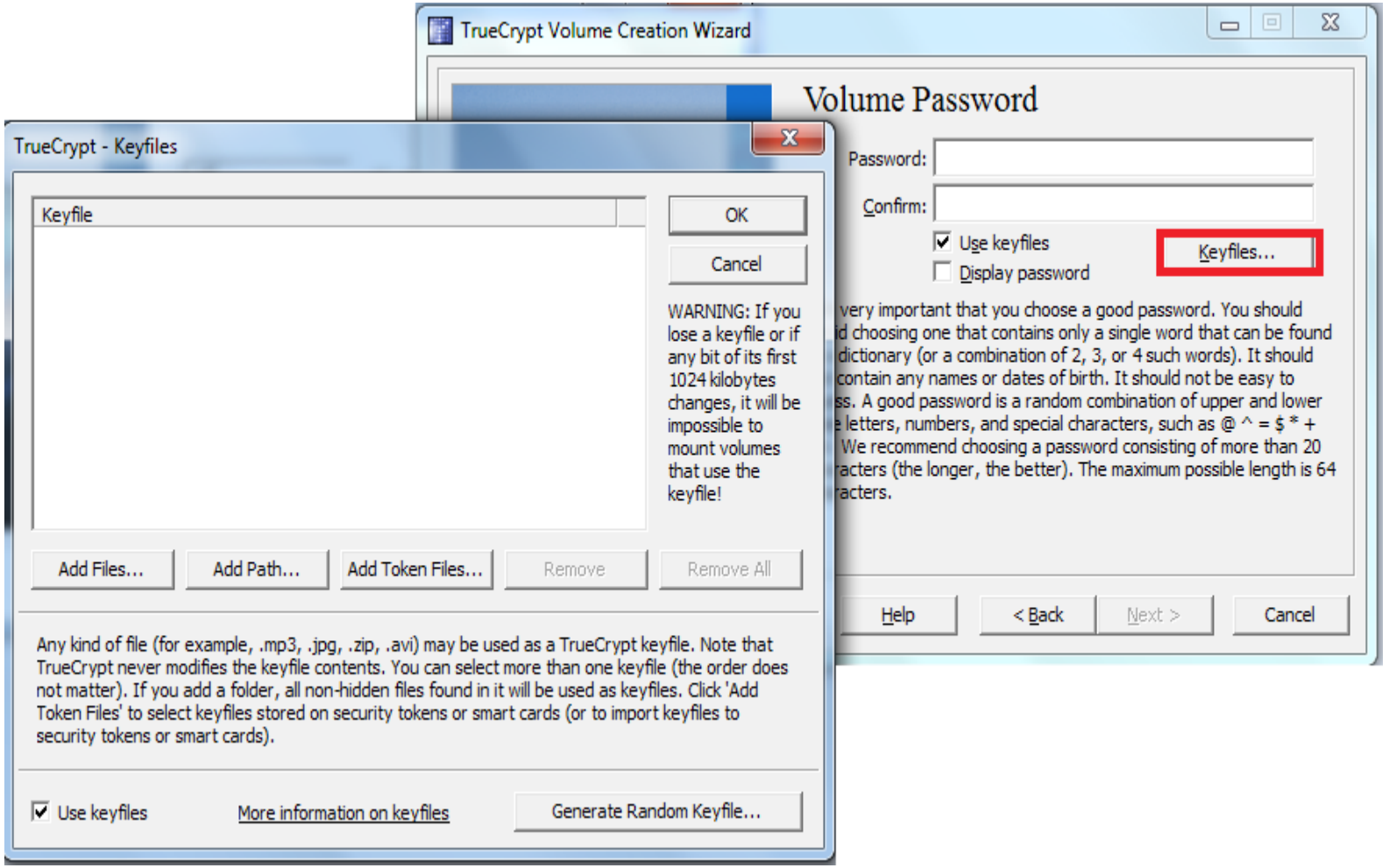
Devices


TrueCrypt Volume Creation Wizard
TRUECRYPT
Encryption Options
Encryption Algorithm
Serpent-Twofish-AES
Test
Three ciphers in a cascade operating in XTS mode. Each block is first encrypted with AES (256-bit key), then with Twofish (256-bit key), and finally with Serpent (256-bit key). Each cipher uses its own key. All keys are mutually independent.
More information
Benchmark
Hash Algorithm
SHA-512
Information on hash algorithms
Help
< Back
Next >
Cancel

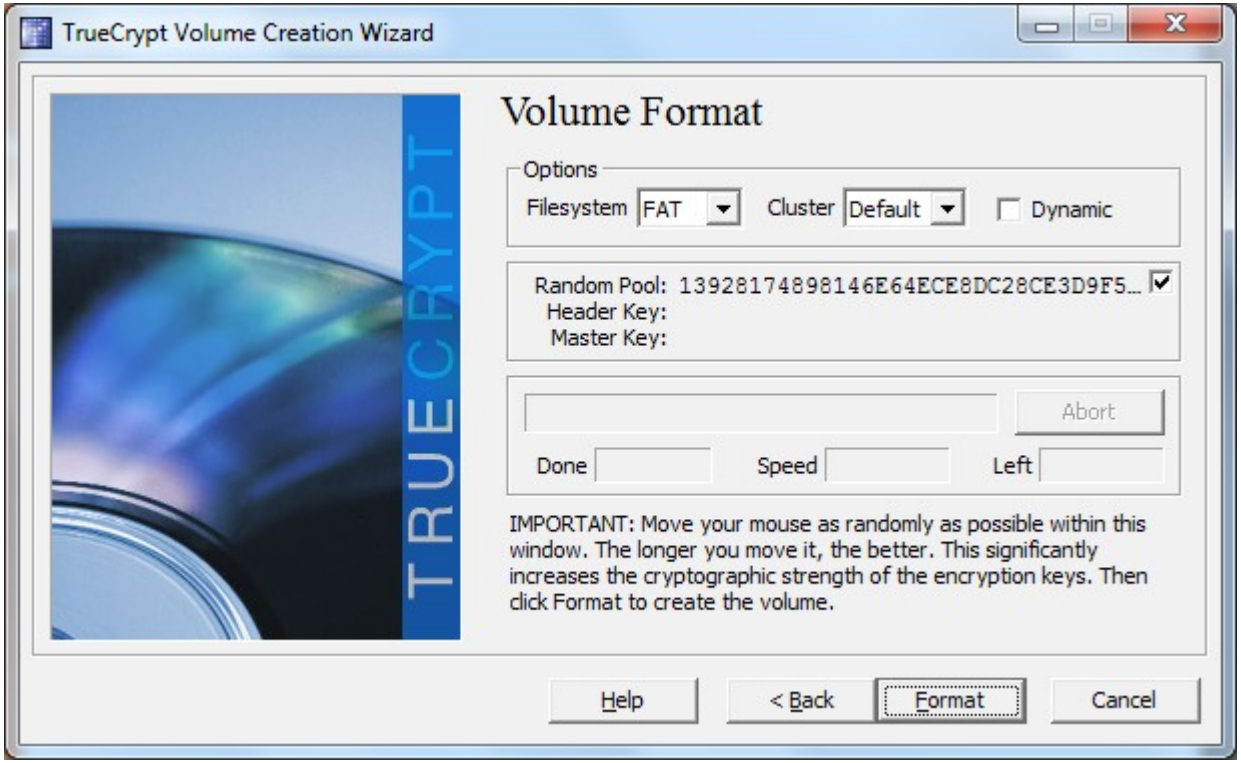
Devices


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Size
10
KB
MB
GB
Free space on drive C:\ is 360.25 GB
Please specify the size of the container you want to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.
Note that the minimum possible size of a FAT volume is 292 KB.
The minimum possible size of an NTFS volume is 3792 KB.
Help
< Back
Next >
Cancel

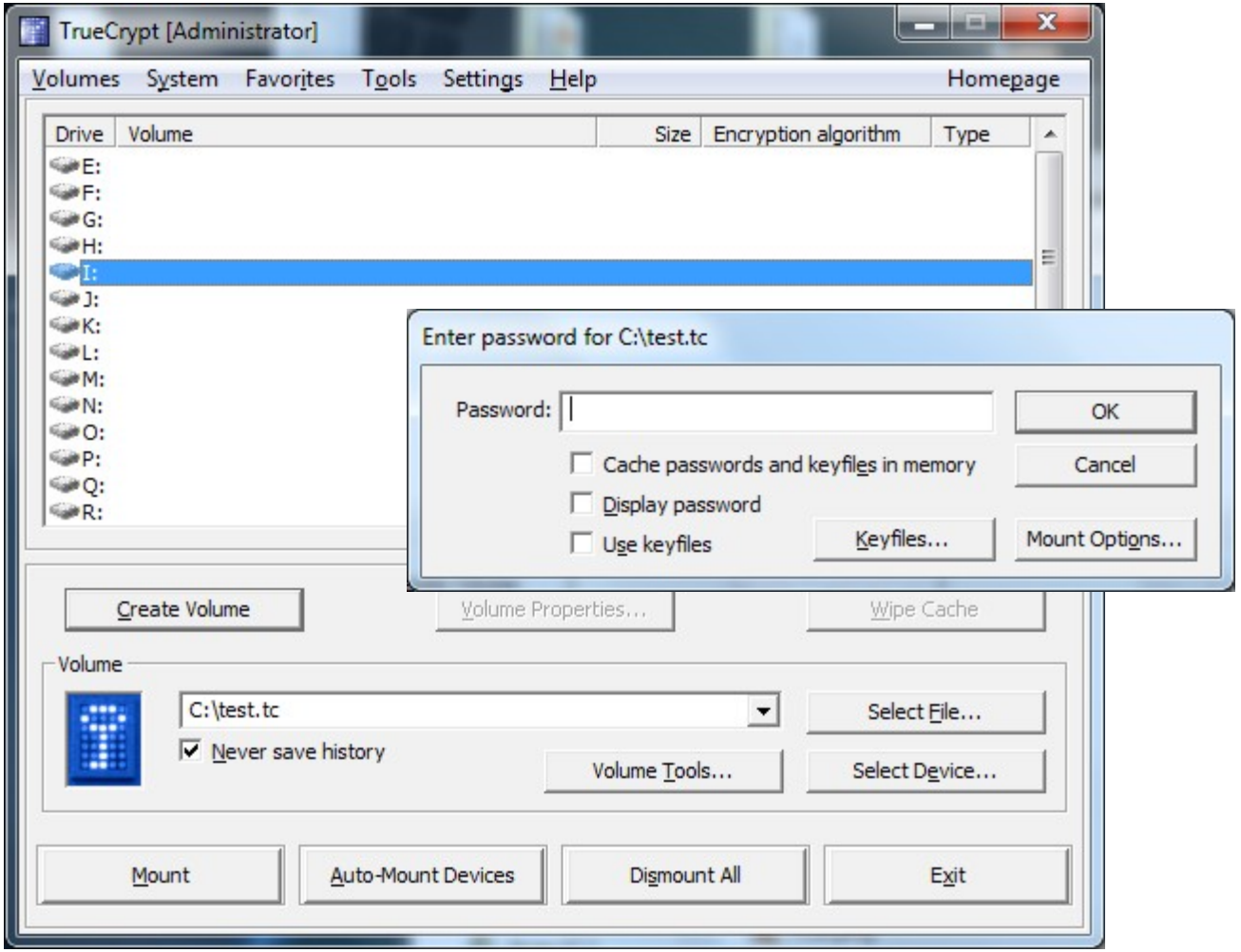
Devices


TrueCrypt Volume Creation Wizard
Volume Password
Password:
Confirm:
Use keyfiles
Display password
Keyfiles...
very important that you choose a good password. You should
id choosing one that contains only a single word that can be found
dictionary (or a combination of 2, 3, or 4 such words). It should
contain any names or dates of birth. It should not be easy to
ss. A good password is a random combination of upper and lower
letters, numbers, and special characters, such as @ ^ = $ * +
We recommend choosing a password consisting of more than 20
racters (the longer, the better). The maximum possible length is 64
racters.
Help
< Back
Next >
Cancel
TrueCrypt - Keyfiles
Keyfile
OK
Cancel
WARNING: If you lose a keyfile or if any bit of its first 1024 kilobytes changes, it will be impossible to mount volumes that use the keyfile!
Add Files...
Add Path...
Add Token Files...
Remove
Remove All
Any kind of file (for example, .mp3, .jpg, .zip, .avi) may be used as a TrueCrypt keyfile. Note that TrueCrypt never modifies the keyfile contents. You can select more than one keyfile (the order does not matter). If you add a folder, all non-hidden files found in it will be used as keyfiles. Click 'Add Token Files' to select keyfiles stored on security tokens or smart cards (or to import keyfiles to security tokens or smart cards).
Use keyfiles
More information on keyfiles
Generate Random Keyfile...

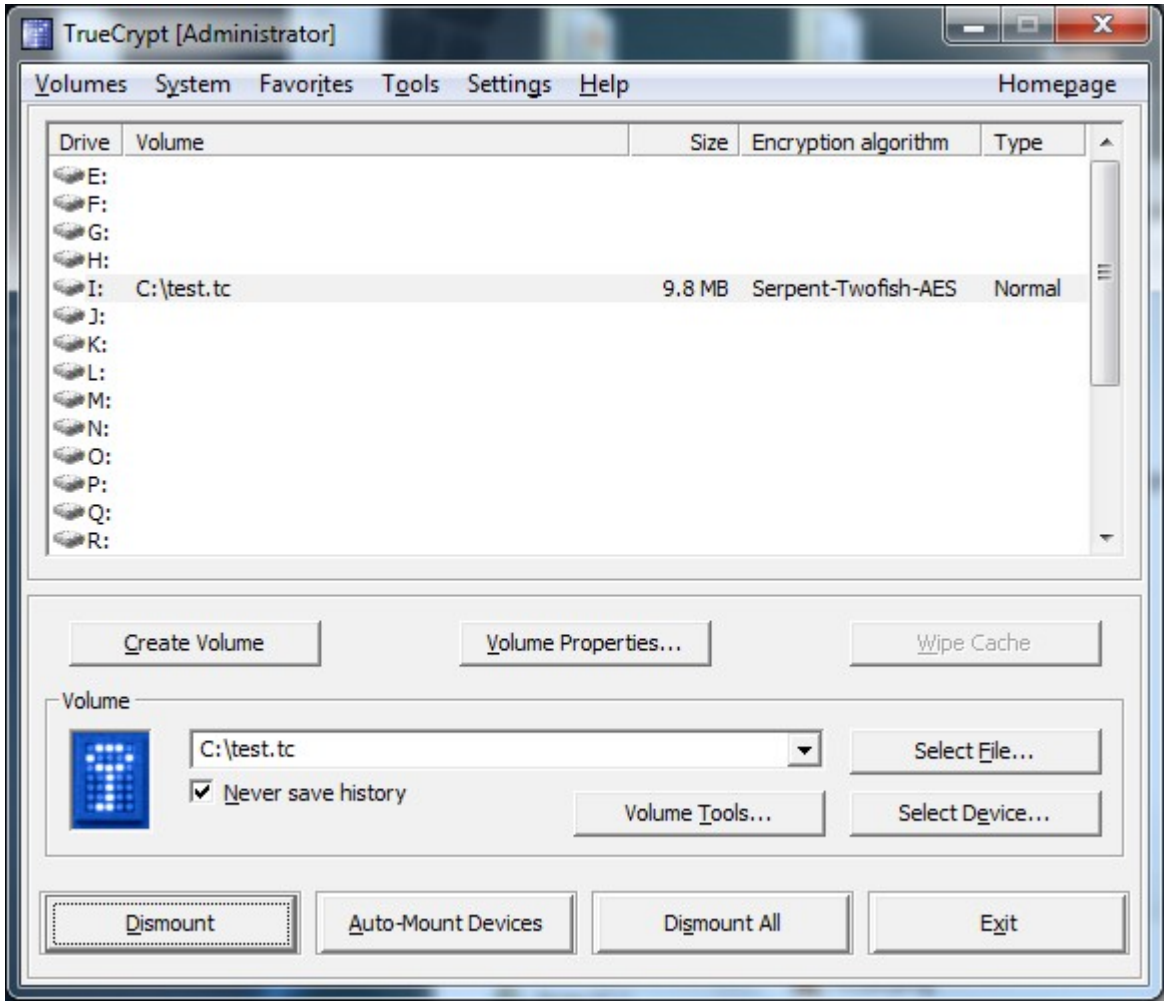
Devices


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Format
Options
Filesystem FAT
Cluster Default
Dynamic
Random Pool: 13928174898146E64ECE8DC28CE3D9F5...
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Back
Format
Cancel

Devices


TrueCrypt [Administrator]
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
Enter password for C:\test.tc
Password:
OK
Cancel
Cache passwords and keyfiles in memory
Display password
Use keyfiles
Keyfiles...
Mount Options...
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\test.tc
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Devices


TrueCrypt [Administrator]
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
E:
F:
G:
H:
I: C:\test.tc 9.8 MB Serpent-Twofish-AES Normal
J:
K:
L:
M:
N:
O:
P:
Q:
R:
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\test.tc
Never save history
Select File...
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

Linksammlung

http://de.wikipedia.org/wiki/Kryptographie

http://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung

http://de.wikipedia.org/wiki/Polyalphabetische_Substitution

http://iPir.at/nigmail

http://www.truecrypt.org/

http://www.cypherpunks.ca/otr/

Danke für Ihre Aufmerksamkeit!

Noch Fragen?