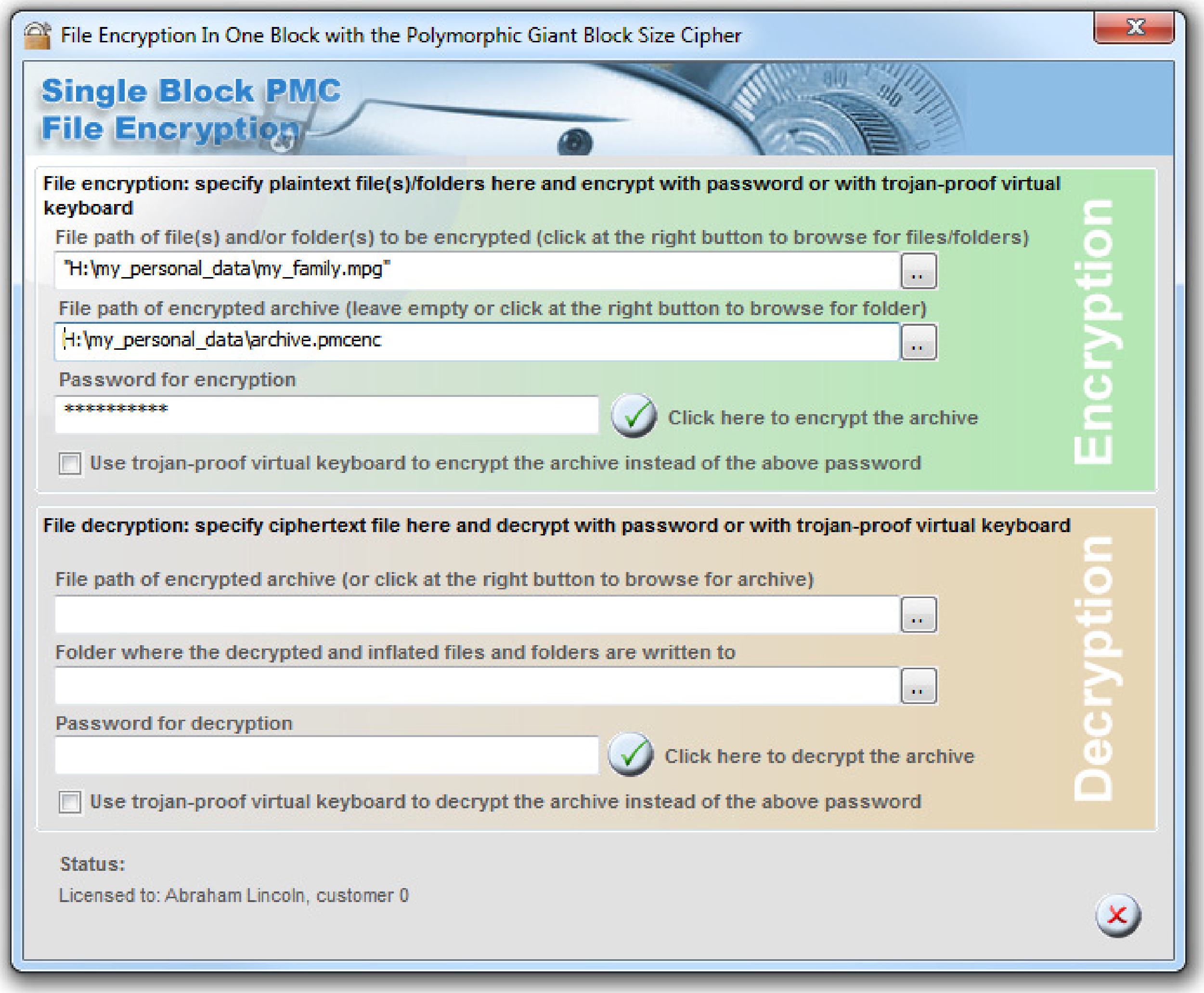


File Encryption In One Block with the Polymorphic Giant Block Size Cipher

File encryption: specify plaintext file(s)/folders here and encrypt with password or with trojan-proof virtual keyboard

File path of file(s) and/or folder(s) to be encrypted (click at the right button to browse for files/folders)

"H:\my_personal_data\my_family.mpg"

File path of encrypted archive (leave empty or click at the right button to browse for folder)

H:\my_personal_data\archive.pmcenc

Password for encryption

****

✓ Click here to encrypt the archive

□ Use trojan-proof virtual keyboard to encrypt the archive instead of the above password

File decryption: specify ciphertext file here and decrypt with password or with trojan-proof virtual keyboard

File path of encrypted archive (or click at the right button to browse for archive)

Folder where the decrypted and inflated files and folders are written to

Password for decryption

✓ Click here to decrypt the archive

□ Use trojan-proof virtual keyboard to decrypt the archive instead of the above password

Status:

Licensed to: Abraham Lincoln, customer 0

"File Encryption In One Block" User Guide

First published: July 2012
This revision: July 2012

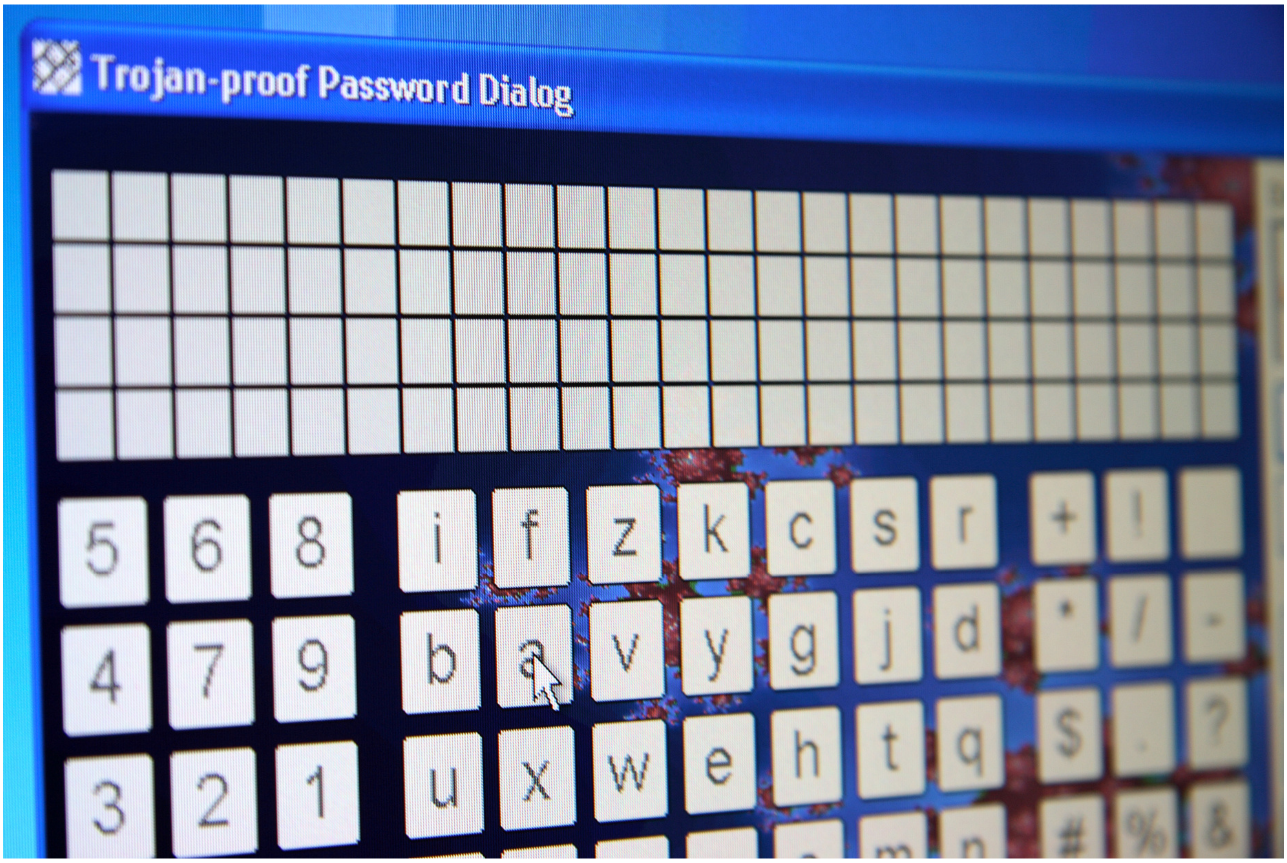
Global IP Telecommunications, Ltd. & PMC Ciphers, Inc. - Josephsburgstr. 85, 81673 Munich, Germany
Tel. +49 89 235 1468-0

"File Encryption In One Block"

Introduction

The idea behind "File Encryption In One Block" is to provide an ultimate encryption tool for files.
The tool is ultimate through the following features:

- An arbitrary amount of files with arbitrary file size is compressed and subsequently encrypted
- The cipher that is used to encrypt data can handle blocks with a length ranging between 16 bytes to 256 Megabytes IN A SINGLE BLOCK. Special versions with 4 Gigabyte block size can be compiled on request. Multiple blocks are encrypted if compressed data exceeds the maximum supported size (>256Mb or >4Gb respectively).
- Passphrases can be entered using a virtual keyboard that is Trojan horse proof. Even if a number of Trojan Horses (i.e. malicious computer viruses that infect a user's computer and that report keystrokes and/or screen content back to the server of a criminal or an intelligence agency) have infected the user's computer, users can still be sure that their password remains completely secret.


Trojan-proof Password Dialog
5 6 8 i f z k c s r + !
4 7 9 b a v y g j d * / -
3 2 1 u x w e h t q $. ?
m n # % &

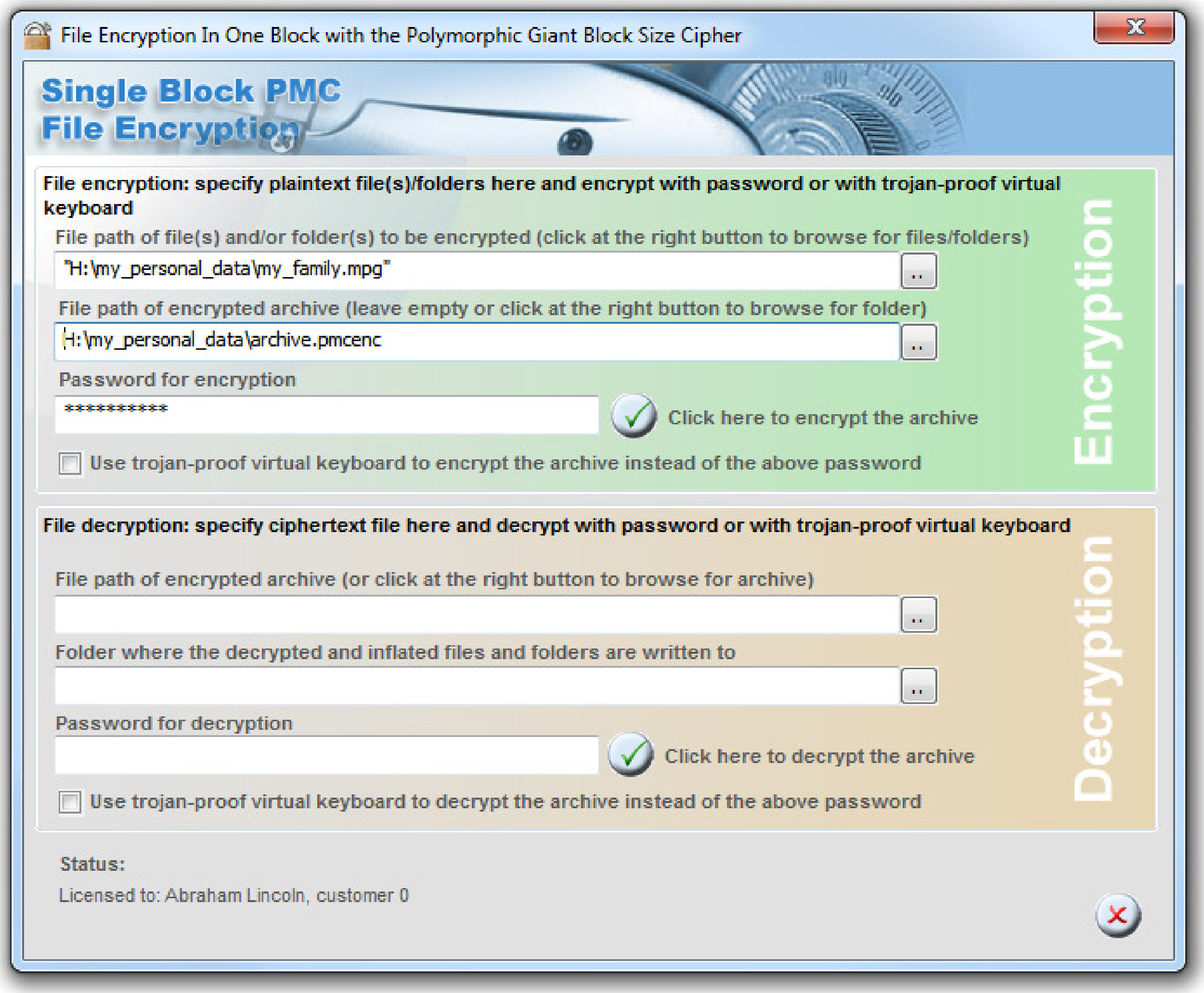
"File Encryption In One Block" and "TurboCrypt" are the very first products of their kind featuring the trojan horse-proof password dialog.

Installation

The tool is not intended to be installed on a computer as this is simply not necessary. This makes the software as versatile as ever possible.
It is although recommended to use the 32 bit version with Microsoft Windows XP (32 bit), Microsoft Windows Vista (32 bit) or Microsoft Windows 7 (32 bit). The 64 bit version only runs on 64 bit Windows versions.

Encryption of data

The user interface of "File Encryption In One Block" is divided into the upper part which provides all the controls that are required to handle data encryption and the lower part which deals with decryption tasks.



File Encryption In One Block with the Polymorphic Giant Block Size Cipher

Single Block PMC File Encryption

File encryption: specify plaintext file(s)/folders here and encrypt with password or with trojan-proof virtual keyboard

File path of file(s) and/or folder(s) to be encrypted (click at the right button to browse for files/folders)

"H:\my_personal_data\my_family.mpg"

File path of encrypted archive (leave empty or click at the right button to browse for folder)

H:\my_personal_data\archive.pmcenc

Password for encryption

****

Click here to encrypt the archive

□ Use trojan-proof virtual keyboard to encrypt the archive instead of the above password

File decryption: specify ciphertext file here and decrypt with password or with trojan-proof virtual keyboard

File path of encrypted archive (or click at the right button to browse for archive)

Folder where the decrypted and inflated files and folders are written to

Password for decryption

Click here to decrypt the archive

□ Use trojan-proof virtual keyboard to decrypt the archive instead of the above password

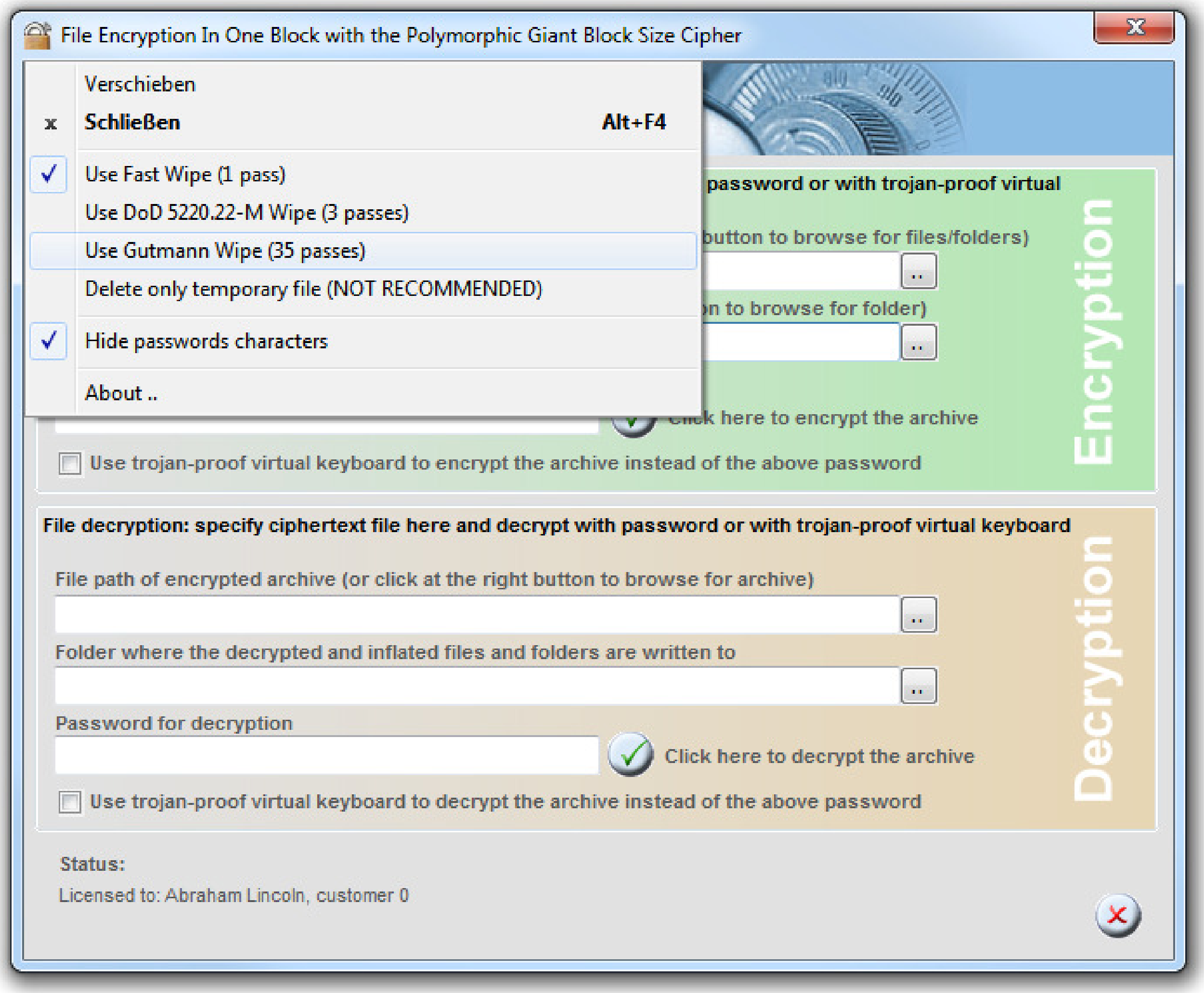
Status:

Licensed to: Abraham Lincoln, customer 0

Simply browse for the files or folders you want to encrypt, then select a file path for the encrypted file archive that is to be created and finally specify a passphrase or set the checkbox next to "Use trojan-proof virtual keyboard .." to the checked state.

To start the encryption process, click at the ✓ (OK) button.

File encryption can be a very lengthy operation. Status information is provided at any time, although. In any case a temporary file residing in the same directory as the encrypted file archive is created. At the end of the encryption operation, this file archive needs to be secure wiped. The default algorithm is "Fast Wipe". More options are available at the program icon:



File Encryption In One Block with the Polymorphic Giant Block Size Cipher

Verschieben

x Schließen Alt+F4

✓ Use Fast Wipe (1 pass)

Use DoD 5220.22-M Wipe (3 passes)

Use Gutmann Wipe (35 passes)

Delete only temporary file (NOT RECOMMENDED)

✓ Hide passwords characters

About ..

password or with trojan-proof virtual

button to browse for files/folders)

n to browse for folder)

ck here to encrypt the archive

□ Use trojan-proof virtual keyboard to encrypt the archive instead of the above password

Encryption

File decryption: specify ciphertext file here and decrypt with password or with trojan-proof virtual keyboard

File path of encrypted archive (or click at the right button to browse for archive)

Folder where the decrypted and inflated files and folders are written to

Password for decryption

Click here to decrypt the archive

□ Use trojan-proof virtual keyboard to decrypt the archive instead of the above password

Decryption

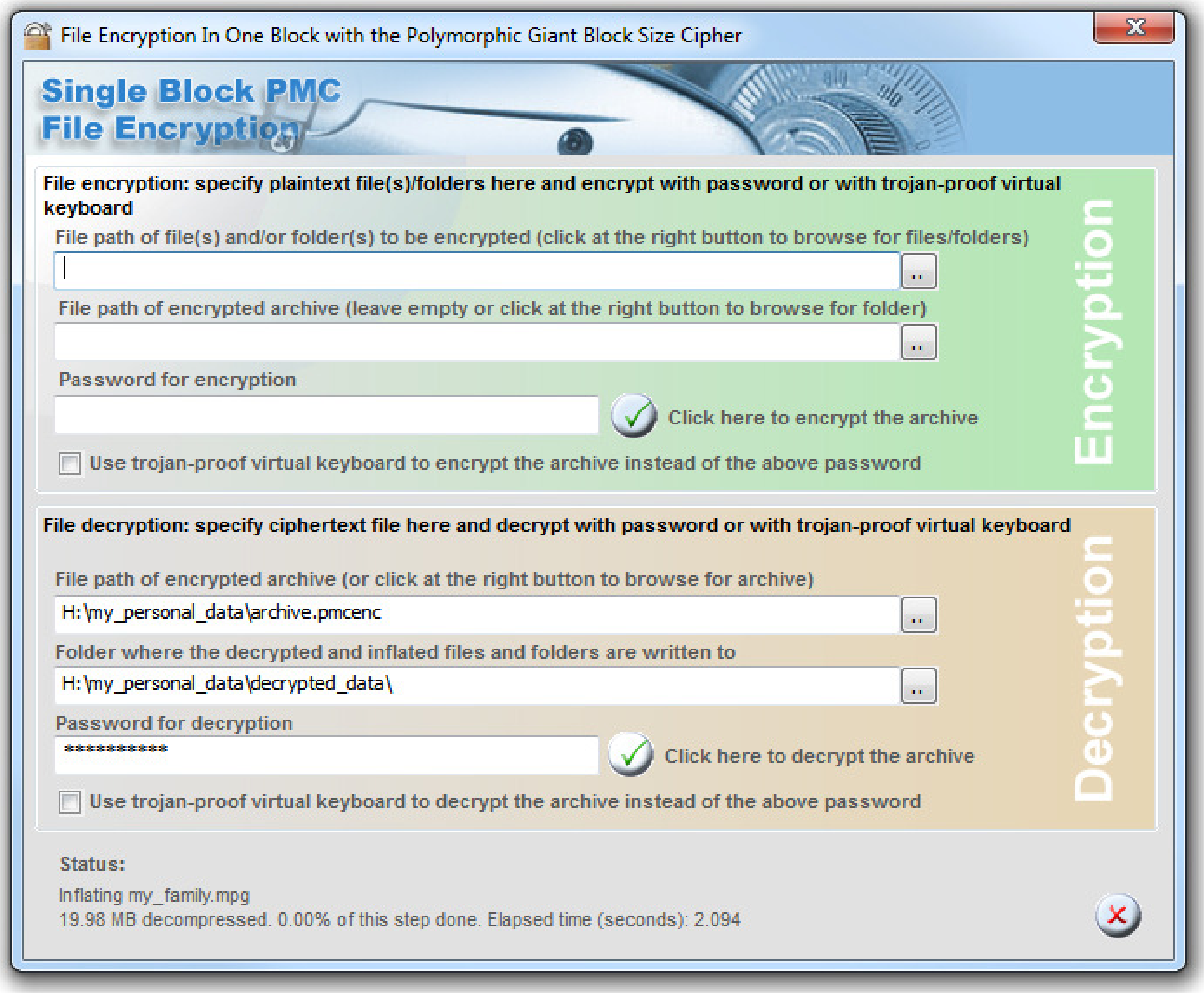
Status:

Licensed to: Abraham Lincoln, customer 0

The recommended wipe method is "Gutmann Wipe". The 35 passes although require a lot of time and in case the data is written to flash memory (e.g. to a USB memory stick or a Solid State Disk), Fast Wipe is recommended in order not to stress the memory chips.

Decryption of data

Only the lower part of the User Interface is needed. Here all controls required for decryption are grouped.



File Encryption In One Block with the Polymorphic Giant Block Size Cipher

Single Block PMC File Encryption

File encryption: specify plaintext file(s)/folders here and encrypt with password or with trojan-proof virtual keyboard

File path of file(s) and/or folder(s) to be encrypted (click at the right button to browse for files/folders)

File path of encrypted archive (leave empty or click at the right button to browse for folder)

Password for encryption

Click here to encrypt the archive

□ Use trojan-proof virtual keyboard to encrypt the archive instead of the above password

File decryption: specify ciphertext file here and decrypt with password or with trojan-proof virtual keyboard

File path of encrypted archive (or click at the right button to browse for archive)

H:\my_personal_data\archive.pmcenc

Folder where the decrypted and inflated files and folders are written to

H:\my_personal_data\decrypted_data\

Password for decryption

****

Click here to decrypt the archive

□ Use trojan-proof virtual keyboard to decrypt the archive instead of the above password

Status:

Inflating my_family.mpg

19.98 MB decompressed. 0.00% of this step done. Elapsed time (seconds): 2.094

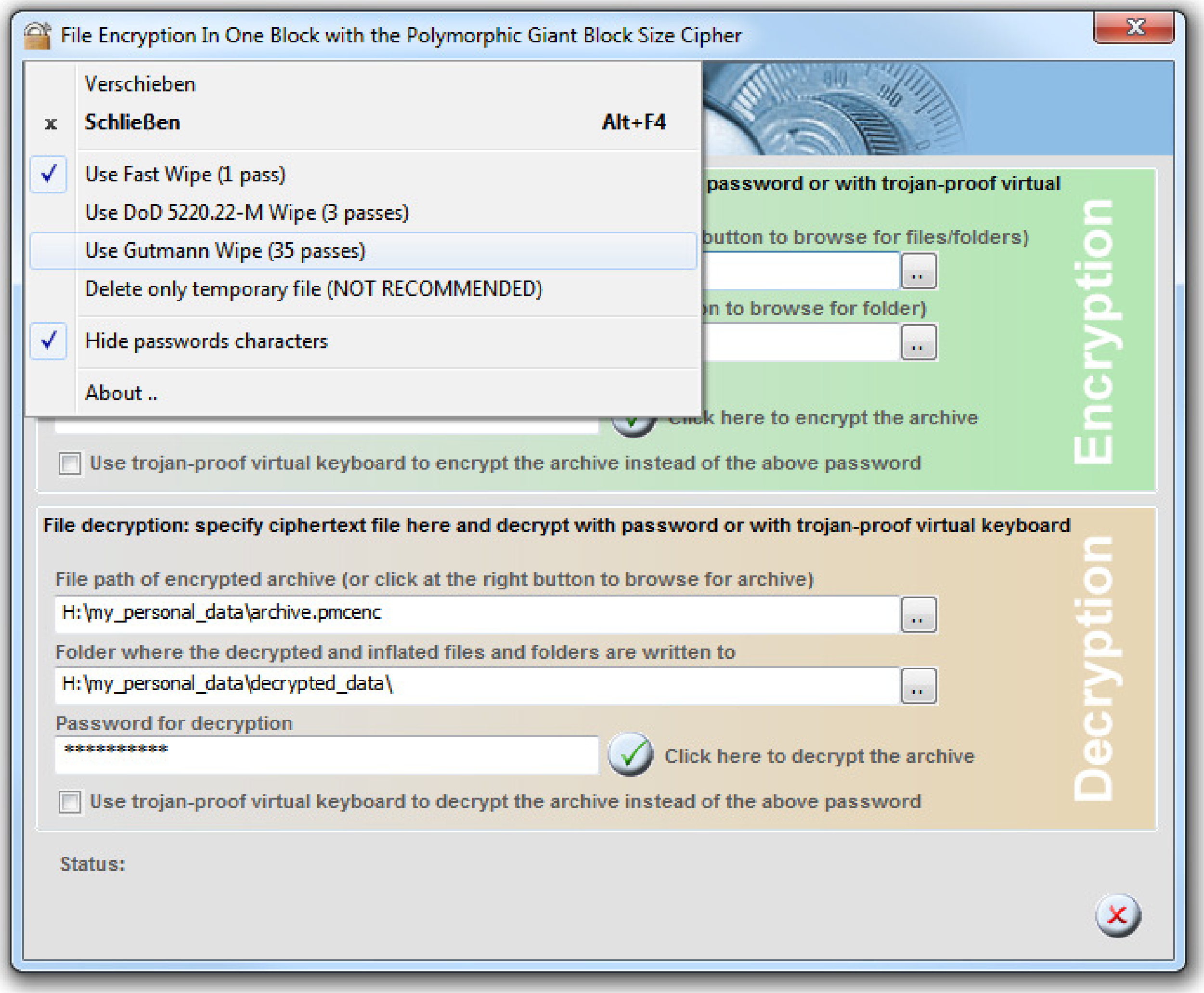
First you need to specify the file path to the encrypted archive that you want to decrypt. Simply browse for the file.

Then specify a folder (directory) where the decrypted data shall be stored by the software.

Finally specify a passphrase or set the checkbox next to "Use trojan-proof virtual keyboard .." to the checked state.

To start the decryption process, click at the ✓ (OK) button. Already existing files are overwritten by the software! It is thus good practice to decrypt data to an empty folder.
The software reconstructs complex file paths of any size. Decryption consequently can take a while. Status information is provided at any time, although.

In any case a temporary file residing in the same directory as the encrypted file archive is created. At the end of the decryption operation, this file archive needs to be secure wiped. The default algorithm is "Fast Wipe". More options are available at the program icon:



File Encryption In One Block with the Polymorphic Giant Block Size Cipher

Verschieben
x Schließen Alt+F4
✓ Use Fast Wipe (1 pass)
Use DoD 5220.22-M Wipe (3 passes)
Use Gutmann Wipe (35 passes)
Delete only temporary file (NOT RECOMMENDED)
✓ Hide passwords characters
About ..
Encryption
Decryption

password or with trojan-proof virtual

button to browse for files/folders)

n to browse for folder)

ck here to encrypt the archive

□ Use trojan-proof virtual keyboard to encrypt the archive instead of the above password

File decryption: specify ciphertext file here and decrypt with password or with trojan-proof virtual keyboard

File path of encrypted archive (or click at the right button to browse for archive)

H:\my_personal_data\archive.pmcenc

Folder where the decrypted and inflated files and folders are written to

H:\my_personal_data\decrypted_data\

Password for decryption

****

Click here to decrypt the archive

□ Use trojan-proof virtual keyboard to decrypt the archive instead of the above password

Status:

The recommended wipe method is "Gutmann Wipe". The 35 passes although require a lot of time and in case the data is written to flash memory (e.g. to a USB memory stick or a Solid State Disk), Fast Wipe is recommended in order not to stress the memory chips.

Command line interface

Provides for encryption/decryption in a single block WITHOUT compression for a single file or WITH compression for multiple files and folders.
File size ranges from 16 bytes to 256MB if data compression is NOT used.

File size ranges from 0 bytes to any practical value IF data compression is used.

The command line can be as long as 32767. If a file is specified, the single file is compressed and encrypted. If a folder is specified, all files and sub-folders are compressed and encrypted.

Max. length of password: 256 characters.

Encryption:

Example: Encryption of a file WITHOUT white spaces (test_video.ts) with password 123456

```
feiob.exe encrypt "e:\video\_test_video.ts" "e:\video\_test_video.pmcenc"
123456
```

or with data compression:

Files and folders can be specified (also very big ones exceeding 4GB). The last file name is the path to the encrypted archive.

A temporary file is created in the same folder where the output file is stored. This file needs to be securely wiped after the encryption process. Default is Fast Wipe (1 pass).
Options:
- wipe_fast (1 pass)
- wipe_dod (DoD 5220.22-M, 3 passes with last pass read-after-write)
- wipe_gutmann (Gutmann wipe, 35 passes).
- delete_only (0 passes, NOT RECOMMENDED AT ALL)

```
feiob.exe encrypt -compress -wipe_fast "e:\video\_test_video.ts" "e:\video\gui-
idea.jpg" e:\video\_test_video.pmcenc 123456
```

Decryption:

Example: Decryption of a file archive WITHOUT data compression with password 123456

```
feiob.exe decrypt "e:\video\_test_video.pmcenc" "e:\video\_test_video.ts"
123456
```

or with data compression:

```
feiob.exe decrypt -inflate "e:\video\_test_video.pmcenc"
"e:\video\folder_for_decrypted_archive" 123456
```

or - in order to specify the secure wipe method:

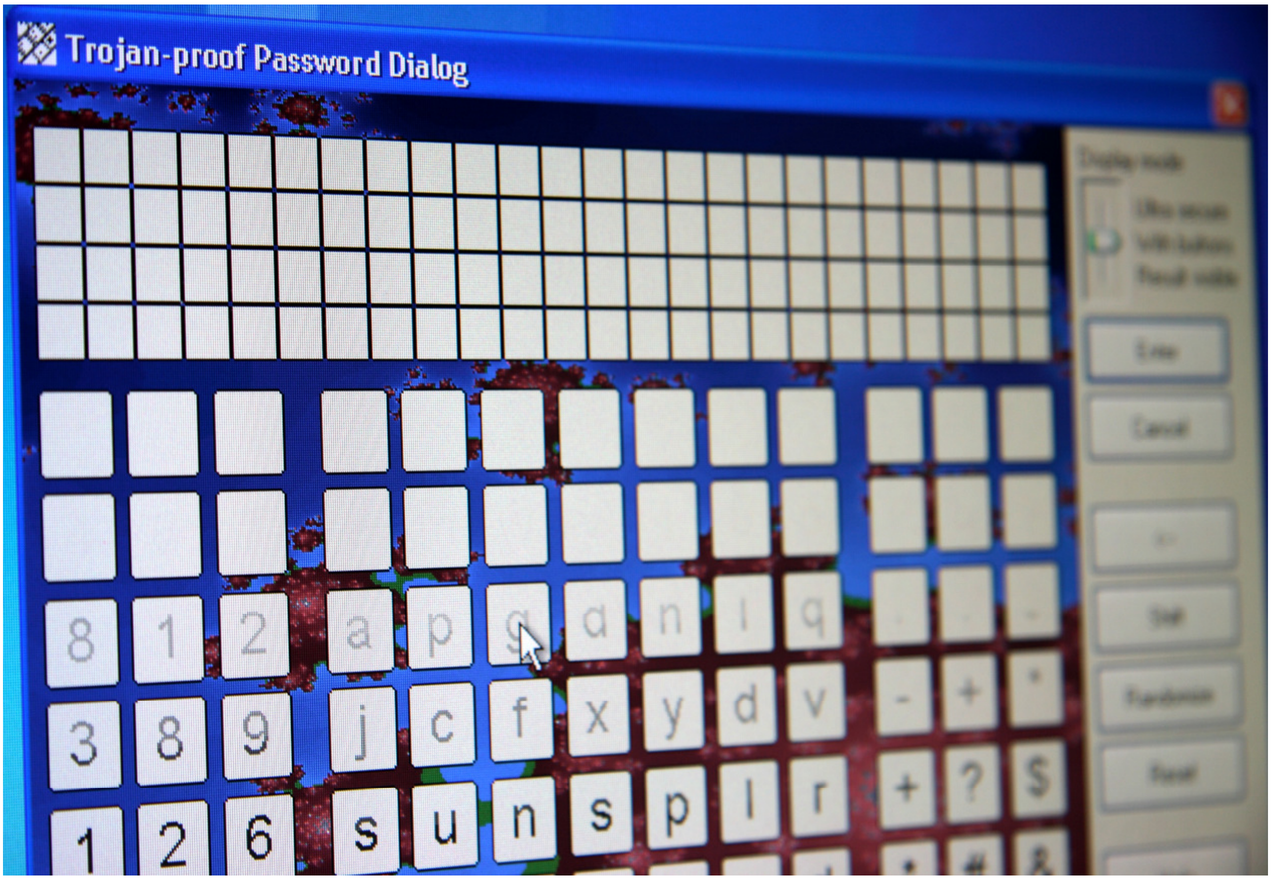
```
feiob.exe decrypt -inflate -wipe_dod "e:\video\_test_video.pmcenc"
"e:\video\_folder_for_decrypted_archive" 123456
```

Wipe options are the same as for encryption:
- wipe_fast (1 pass)
- wipe_dod (DoD 5220.22-M, 3 passes with last pass read-after-write)
- wipe_gutmann (Gutmann wipe, 35 passes).
- delete_only (0 passes, NOT RECOMMENDED AT ALL)

Background information

Trojan-horse-proof virtual keyboard

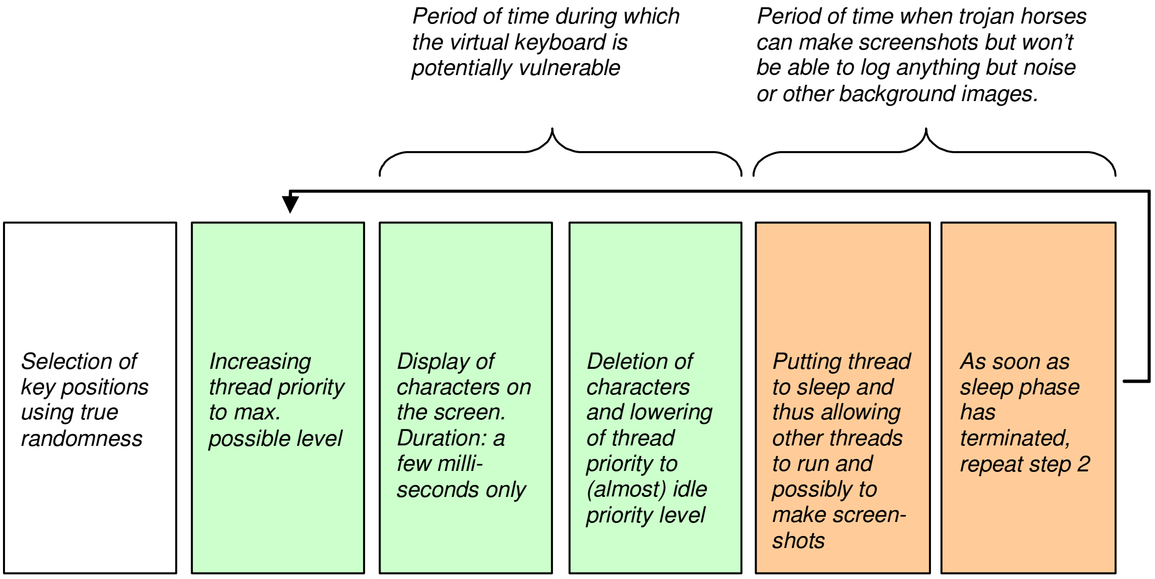
The photo below shows our invention of a virtual keyboard that allows for totally secure password entry. Conventional encryption software only allows for password entry by keyboard (or by smart cards and other authentication methods that are not suitable for guaranteeing perfect secrecy). Keystrokes can either be recorded or transmitted by a hidden piece of hardware in the keyboard or they are simply logged by malicious software – so called “Trojan Horses”. While normal criminals sometimes use the first approach do professional hackers and states generally prefer the latter approach.



In any case does our invention provide perfect secrecy for your passwords as the trojan-horse-proof virtual keyboard does not allow any malicious piece of software to gather any useful information.

The photo actually reveals the mode of operation of the virtual keyboard. Key characters are drawn, deleted, drawn again and deleted again. This sequence repeats itself several times per second. In order to keep highly intelligent trojan horses from taking a snapshot of the screen while all characters are visible, a characteristic that is inherent to the task scheduler, which is implemented in the core of the operating system, is exploited:
Processes running at realtime priority level will probably never be descheduled by processes featuring a lower priority level. Even processes with the same (very high) priority level won’t interrupt our virtual keyboard process as long as the virtual keyboard does not consume too much CPU time. It wouldn’t make must sense for the scheduler to interrupt a media player application by a process that e.g. indexes e-mails in the background. The operating system wouldn’t be popular if audio or video playback was choppy.

Sequence of operations executed by the trojan-horse-proof virtual keyboard:


Period of time during which the virtual keyboard is potentially vulnerable
Period of time when trojan horses can make screenshots but won't be able to log anything but noise or other background images.
Selection of key positions using true randomness
Increasing thread priority to max. possible level
Display of characters on the screen. Duration: a few milli-seconds only
Deletion of characters and lowering of thread priority to (almost) idle priority level
Putting thread to sleep and thus allowing other threads to run and possibly to make screen-shots
As soon as sleep phase has terminated, repeat step 2

It should be noted that modern microprocessors feature at least two independent CPU cores. TurboCrypt uses up all available additional CPU cores to compute pseudorandom numbers in order not to give any malicious piece of software any access to CPU time.

This fascinatingly simple but highly efficient method to keep hackers away from your password data has been thoroughly tested many times. You can test the efficiency easily by yourself with the help of a frame grabber tool.

For more information: http://www.pmc-ciphers.com

This is a preliminary document and may be changed substantially prior to final commercial release. This document is provided for informational purposes only and PMC Ciphers & Global IP Telecommunications make no warranties, either express or implied, in this document. Information in this document is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of PMC Ciphers or Global IP Telecommunications.

PMC Ciphers or Global IP Telecommunications may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from PMC Ciphers or Global IP Telecommunications, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.