Chiasmus™ for Windows/Linux

Description

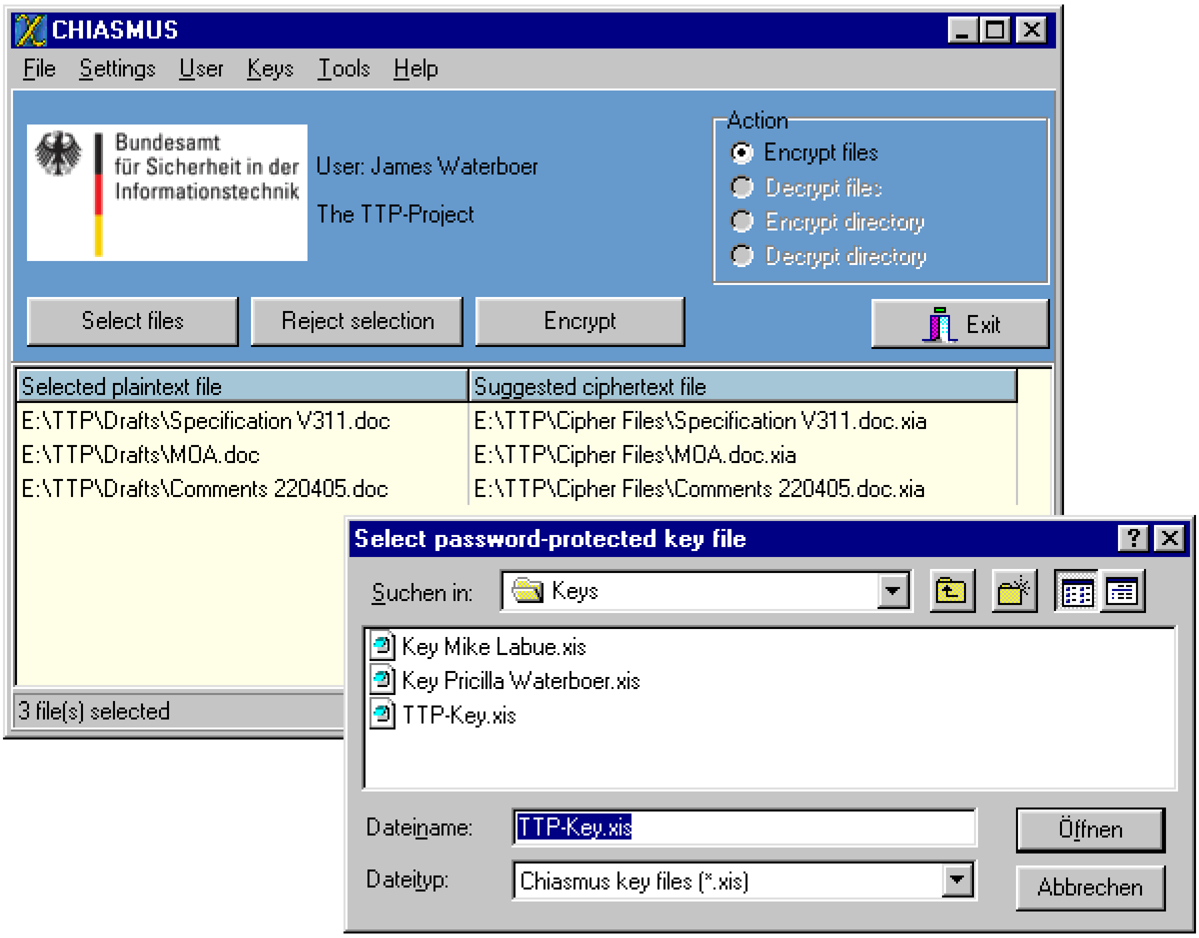
Chiasmus™ is an encryption program for Windows (Windows 95, 98, 2000, ME, NT 3.5.2 and higher, XP, Vista, 7, 8) and Linux. Chiasmus is a 32-bit application, but it also runs on newer 64-bit operating sytsems (Windows 7, 8 and Linux). With Chiasmus it is possible to encrypt individual files or entire folders.

The built-in random number generator enables you to generate keys yourself. However, keys previously exchanged with communications partners can also be used. The keys can either be read from a file or else entered over the keyboard.

Chiasmus is easy to install. During installation, no entries are added either to the Start menu or the registry, or to any other system directories. The software does not use any system drivers or DLLs either. On the other hand, Chiasmus does not embed itself into any other applications (Word, Excel, Access, Lotus Notes, etc.). This rules out the possibility of transparent encryption of application data in the background. Encryption and decryption of files or folders must always be initiated by the user in a separate operation.

The Chiasmus software product is subject to greater risks than a hardware solution. With a PC that is connected to the internet, it is possible that protection could not be provided to the extent required. The protection requirement of the information to be protected should therefore be no higher than "moderate".

Chiasmus is available as a Windows program with a graphical user interface and as a command-line-based Linux program. The Windows program is switchable from German to English language. The Linux program is availabel in German language only.



User: James Waterboer

The TTP-Project

Action
- ● Encrypt files
- ○ Decrypt files
- ○ Encrypt directory
- ○ Decrypt directory

Selected plaintext file	Suggested ciphertext file
E:\TTP\Drafts\Specification V311.doc	E:\TTP\Cipher Files\Specification V311.doc.xia
E:\TTP\Drafts\MOA.doc	E:\TTP\Cipher Files\MOA.doc.xia
E:\TTP\Drafts\Comments 220405.doc	E:\TTP\Cipher Files\Comments 220405.doc.xia

3 file(s) selected

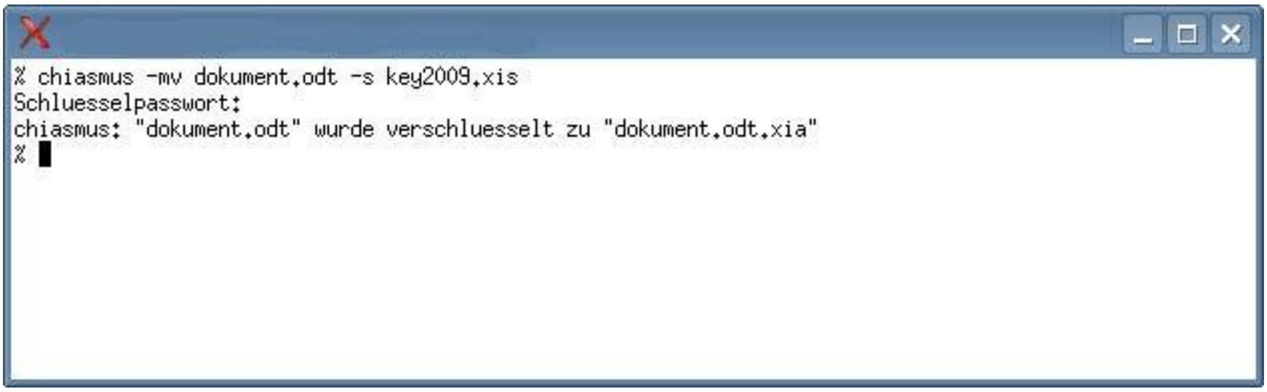
Suchen in: Keys

- Key Mike Labue.xis
- Key Pricilla Waterboer.xis
- TTP-Key.xis

Dateiname: TTP-Key.xis

Dateityp: Chiasmus key files (*.xis)

Figure: Chiasmus for Windows in operation



```
% chiasmus -mv dokument.odt -s key2009.xis
Schluesselpasswort:
chiasmus: "dokument.odt" wurde verschluesselt zu "dokument.odt.xia"
% 
```

Figure: Chiasmus for Linux in operation. The Chiasmus user has enciphered the file dokument.odt with the keyfile key2009.xis. The password is not displayed on the screen.

Cryptographic details

The core of the program is the BSI's own symmetric block encipherment algorithm, Chiasmus. Chiasmus was specifically developed for software implementations. Chiasmus encrypts 64-bit blocks into 64-bit blocks, using a 160-bit key. Chiasmus for Windows/Linux uses Chiasmus in cipher block chaining (CBC) mode. The effective key length is 128 bits, the remaining 32 bits constituting a checksum.